前　言

初等数论是研究整数性质的一个数论分支，它是数学中历史悠久的分支之一。早在公元前3世纪，古希腊数学家欧几里德(Euclid)就已证明了猜想"有无穷多个素数存在"的正确性。我国古代的《孙子算经》中给出了求解一次同余式组的算法——孙子定理，亦称中国剩余定理。1801年，数学家高斯(Gauss)在其著作《算术研究》中首先提出了二次互反律、原根存在的充分必要条件等重要结果，并对同余理论做了较为系统的研究。通常，高斯的这一名著被认为是数论作为数学的一个独立分支的标志。

古老悠久的数论在数学发展史中占据着不容忽视的一页，不少重大数论课题的研究都创造了极其深刻的新的方法，甚至促进着新的数学分支的发展。例如对不定方程和高次互反律的研究促进了代数数论与类域论的发展。20世纪以来，人们惊喜地发现：初等数论在当代计算机科学、组合数学、代数编码、信号的数字处理等科学技术领域得到了极其广泛的应用。时至今日，这一古老学科的底蕴仍然洋溢着诱人的青春活力。

初等数论是一门十分重要的基础课。它不仅应该是高等师范院校数学专业、大学数学各专业的必修课，而且也是计算机科学等许多相关专业所需要的课程。初等数论在离散数学以及计算机科学等诸多学科中所起的日益明显的重要作用绝非偶然。事实上，近代数学中许多重要思想、概念、方法与技巧都源于对整数性质的深入研究而不断丰富和发展起来的。学习初等数论不仅可以掌握它的基本观点、内容和方法，还可以从中领悟某些近代数学思想与方法的背景。

“数学是思维的体操”,初等数论是一门绝好的思维训练课程,由于学习初等数论不需要更多的预备知识,因此学习者主要应学习理论并用以解决一些难度较大的问题。思维是智力与能力的核心,初等数论为学习者提供了开发智力与增长能力的系统素材,它不失为一门思维训练课程。被誉为“世界青年智能大赛”的国际数学奥林匹克(IMO)的试题中,数论或与数论相关的试题占总试题的40%左右,这个结果恰好支持了我们的观点。

正基于此,自1988年以来,我为我的三个不同专业方向的六届硕士研究生都开设了“数论基础”课程。“数论基础”在理论上保持了初等数论的主体结构,在内容上加大了思维训练的强度。与通常的大学本科的“初等数论”不同的是在“数论基础”中直接引用了IMO或世界各国的数学奥林匹克试题。希望这样的课程设计更能适应高等师范院校的研究生与本科生的需求。

全书共分七章。第一章重点介绍初等数论的基础—整除理论。为使读者对整数有一个清楚、正确的认识,本章引入时介绍了自然数的基数理论与序数理论。第二章介绍初等数论发生、发展的原始方法——带余除法与算术基本定理。第三章介绍高斯函数[x],{x}的基本性质与相应的技巧与方法。第四章不定方程与第五章同余的理论与应用是初等数论的最基本的内容。第六章欧拉定理与威尔逊定理介绍了有关定理在二次同余方面的应用。第七章专题选讲重点介绍有关基本概念、方法的引伸与拓广。全书注意到奥林匹克数学的理论与实践的结合,适当地引入了数论的概念、方法在数学奥林匹克领域的应用。

作为“奥林匹克数学的理论与实践”方向的硕士课程建设,初始的讲稿历经几届学生的整理、研讨与反复修改,初步形成了一定的体系。其中,鲍敬谊整理了前五章的讲稿,王蓓演算、核实了前五章的全部习题,倪斯杰负责初稿的部分章、节的审定与修改,李景华、顿继安的硕士论文充实了第七章的部分内容。数论基础的初稿分别由倪斯杰、鲍敬谊、王蓓、兰英、李景华、顿继安各主持一

章的研讨与修改，最后由我终审、定稿。

尽管我们的工作是努力的，数论基础课程的设计尚有一定的新意。但我们深知就我们的力量及短短十余年的时间，要使教材达到预期的目标是很难的。为适应当前教学的需要，权抛“数论基础”为砖，期待更多的“碧玉”问世。

本书可作为高等学校教师、研究生、学生的教学参考用书，也可作为中、小学教师继续教育与进修提高的指导用书。

感谢诸多同仁对本书内容的建议与指导，感谢北京科技出版社领导及刘长梅编辑为本书出版付出的辛勤劳动。

张君达

2002 年 6 月 1 日

目　　录

第一章　整除……………………………………………… (1)
§1　自然数 ……………………………………………… (1)
1.1　自然数与整数 ……………………………………… (1)
1.2　最小数原理 ………………………………………… (4)
1.3　鸽笼原理 …………………………………………… (7)
§2　整除……………………………………………… (11)
2.1　约数和倍数……………………………………… (11)
2.2　基本性质……………………………………… (12)
2.3　数的奇偶性……………………………………… (13)
§3　素数与合数……………………………………… (18)
3.1　素数与合数概念………………………………… (18)
3.2　性质……………………………………………… (19)
3.3　逐步淘汰原则…………………………………… (23)
第二章　算术基本定理 ………………………………… (34)
§1　带余除法……………………………………… (34)
1.1　带余除法……………………………………… (34)
1.2　整数的分类……………………………………… (36)
1.3　P 进制……………………………………………… (38)
§2　最大公约数和最小公倍数……………………… (41)
2.1　最大公约数和最小公倍数……………………… (41)
2.2　辗转相除法……………………………………… (44)
2.3　$ab=(a,b)[a,b]$ ………………………………… (48)
§3　算术基本定理……………………………………… (52)
3.1　算术基本定理……………………………………… (52)

3.2 正约数的个数……………………………………………… (54)
3.3 正约数的和与积……………………………………………… (58)
第三章 竞赛中的几个典型问题 ……………………………… (63)
§1 高斯函数[x]、{x} ……………………………………… (63)
§2 基本性质 ……………………………………………… (63)
§3 技巧与方法 ……………………………………………… (73)
第四章 不定方程 ……………………………………………… (82)
§1 基本概念 ……………………………………………… (82)
1.1 定义 ……………………………………………… (82)
1.2 ax + by = c 的特解和通解……………………………… (83)
§2 一次不定方程 ……………………………………………… (84)
2.1 方程 ax + by = c 的有关算法……………………………… (84)
2.2 性质定理……………………………………………… (86)
2.3 多元线性不定方程……………………………………… (89)
§3 二次或二次以上的不定方程 ……………………………… (95)
3.1 $x^2 + y^2 = z^2$ ……………………………………… (95)
3.2 无穷递降法……………………………………………… (99)
3.3 高次不定方程 ……………………………………… (103)
第五章 同余……………………………………………… (108)
§1 同余……………………………………………… (108)
1.1 同余的概念 ……………………………………… (108)
1.2 同余的等价命题 ……………………………………… (109)
§2 同余的性质……………………………………………… (114)
§3 同余类与代表元……………………………………… (121)
3.1 基本概念 ……………………………………………… (121)
3.2 剩余系的结构与性质 ……………………………… (127)
第六章 欧拉定理与威尔逊定理……………………………… (137)
§1 欧拉函数 ……………………………………………… (137)
1.1 基本概念 ……………………………………………… (137)

1.2　欧拉函数的计算 …………………………………… (137)
1.3　欧拉函数的基本性质 ………………………………… (140)
§2 欧拉定理与威尔逊定理………………………………… (146)
2.1　费尔马(Fermat)定理 ……………………………… (146)
2.2　欧拉(Euler)定理 …………………………………… (151)
2.3　威尔逊定理 ………………………………………… (153)
第七章　专题选讲……………………………………… (158)
§1　枚举与筛选 ……………………………………………… (158)
1.1　有关概念 …………………………………………… (158)
1.2　基本方法与技巧 …………………………………… (159)
§2　集合、分划与整数分拆…………………………………… (165)
2.1　概念 ………………………………………………… (165)
2.2　基本方法 …………………………………………… (168)
2.3　一类自然数集的分划 ……………………………… (172)
§3　整数集的划分 …………………………………………… (179)
3.1　元素已知的整数集的划分 ………………………… (179)
3.2　整数集划分的和性原理 …………………………… (181)
3.3　整数集划分的积性原理 …………………………… (183)
3.4　特殊子集的划分原则 ……………………………… (184)
3.5　应用抽屉原理的划分 ……………………………… (186)
§4　数论在密码上的应用 …………………………………… (187)
4.1　仿射加密法 ………………………………………… (189)
4.2　RSA 系统 …………………………………………… (191)
4.3　MH 系统 …………………………………………… (192)
§5　Nim 对策问题 …………………………………………… (194)
5.1　二进制与 Fibonacci 数列 ………………………… (196)
5.2　Bouton 对策问题 …………………………………… (203)
5.3　Wythoff 对策问题 ………………………………… (208)
5.4　应用举例 …………………………………………… (213)

第一章　整　　除

§1　自然数

1.1　自然数与整数

自然数具有两方面的意义，一表示数量（多少个），一表示次序（第几个）。基数理论与序数理论就是由此而抽象出来的两种主要的自然数理论。

1. 基数理论

基数理论是通过集合与映射等概念建立起来的自然数理论，对有限集来说，等价集合的共同特征是它们的元素个数相同，可以利用这一共同特征的集合进行分类，凡等价集合都归入一类，用一个符号表示它。据此，采用集合论的观点可以给出自然数的定义。

定义 1.1　一切等价集合的共同特征叫做基数

定义 1.2　非空有限集合的基数叫做自然数

若认为自然数包括零，则可不加"非空"条件，在此基础上，可以进一步给出自然数集合的大小关系、加法运算和乘法运算。

定义 1.3　设（非空）有限集合 A 和 B 的基数分别是 a 和 b，当

(1) $A\sim B$ 时，则说 a 等于 b，记作 $a=b$；

(2) $A\sim B'\subset B$，则说 a 小于 b，记作 $a<b$；

(3) $A\supset A'\sim B$，则说 a 大于 b，记作 $a>b$.

定义 1.4　设 $A\cap B=\phi$，$A\cup B=C$，如果（非空）有限集合 A、B、C 的基数分别是 a、b、c，则把 c 叫做 a 与 b 的和，记作 $c=a+b$，a 和 b 叫做加数，求两数和的运算叫做加法。

定义 1.5　设 b 个（非空）有限集 A_1、A_2……A_b 的基数都是

a，且 $A_i \cap A_j = \phi, 1 \leqslant i < j \leqslant b$，如果 $A_1 \cup A_2 \cup \cdots\cdots \cup A_b = c$，则称集合 c 的基数 c 为 a 与 b 的积，记作 $a \times b = c$，a 叫做被乘数，b 叫做乘数。求两数积的运算叫做乘法。

在此基础上，先利用集合的知识论证和与积在自然数集中存在且唯一，以及基本运算定律和基本顺序律成立，然后再利用逆运算来定义减法与除法。在自然数集中讨论减法与除法可以实施的条件是必要的，至于四则运算的其它性质则可以用逻辑推理的方法给出。这样，可以建立并逐渐完善自然数基数理论系统。

2. 序数理论

序数理论是采用公理化方法建立起来的自然数理论。它从两个原理概念：集合与后继以及四条公理出发，确立多种命题，从而建立自然数的理论系统。

定义 1.6 任何一个非空集合 N 的元素叫做自然数，若在 N 中的某些元素间有一个基本关系“后继”(记为“′”)，且满足下列公理：

(1) 存在一个元素，记作 1，它不后继于任何元素(即 $1 \in N$，且若 $a' \in N$，则 $a' \neq 1$)

(2) 对任何元素 a，有且仅有一个后继元素 a'(即若 $a = b$，则 $a' = b'$)。

(3) 除 1 以外，任何一个元素仅能是一个元素的后继元素(即若 $a' = b'$，则 $a = b$)

(4) (归纳公理)若 N 的任一子集 M，满足条件：

① $1 \in M$

② 每当 $k \in M$，就有 $k' \in M$，那么 M 含有一切自然数。

自然数定义的四个公理中，前三个公理的论断是很明显的，公理 4 通常称为归纳公理，由此可以导出一个重要的证明方法——数学归纳法。

应用公理化的方法还可以定义自然数的加法和乘法。

定义 1.7 在自然数集中，运算“+”叫做自然数的加法，应满

足：

(1) 对任何自然数 a，有 $a+1=a'$

(2) 对任何自然数 a 和 b，有 $a+b'=(a+b)'$；数 a 和 b 叫做加数，而相加的结果 $a+b$ 称为和。

定义 1.8 在自然数集中，运算"·"叫做自然数的乘法，应满足：

(1) 对任何自然数 a，有 $a\cdot 1=a$；

(2) 对任何自然数 a 和 b，有 $a\cdot b'=a\cdot b+a$，数 a 叫做被乘数，数 b 叫做乘数，而相乘的结果 $a\cdot b$ 叫做积。

定义 1.9 设 a、b 是自然数，若存在一个自然数 k，使 $a=b+k$ 成立，则说 a 大于 b，记作 $a>b$；或者说 b 小于 a，记作 $b<a$。

由此可论证关于自然数的基本顺序定律是成立的，再从逆运算的角度引入减法与除法及其相应的性质与运算定律，那么自然数的序数理论系统就相应建立并趋于完善。

基数理论与序数理论从两个不同侧面刻画了自然数的意义，并建立了统一的运算法则。

自然数又叫正整数，正整数、0 和负整数统称为整数，通常用 Z 表示整数集，N 或 Z^+ 表示自然数集，全体整数对加法构成了一个 *Abel* 群——$(Z,+,0)$，即满足下列性质：

(1) $\forall a,b\in Z$，有 $a\pm b\in Z$

(2) 结合律：$(a+b)+c=a+(b+c)$ a、b、$c\in Z$

(3) 交换律：$a+b=b+a$，$a,b\in Z$

(4) 有单位元 0：$a+0=a$，$a\in Z$

(5) $\forall a\in Z$，$\exists b\in Z$，使得 $a+b=0$，b 即为 a 的逆元，记作 $-a$。

同时，整数集对乘法运算封闭，即 $\forall a$、$b\in Z$，$a\times b\in Z$，但 $a\div b$ 不一定属于 Z，乘法常简记为 $a\cdot b$ 或 ab。乘法运算满足以下性质：

(1) 结合律：$(ab)c=a(bc)$

(2) 交换律:$ab = ba$

(3) 分配律:$(a+b)c = ac + bc$

(4) $\forall a \in Z$,存在单位元1,使 $a \cdot 1 = a$

由以上性质可知$(Z, +, \cdot, 0, 1)$构成一个可换群。

1.2 最小数原理

定理 1.1 (最小数原理):任意一个自然数的非空子集中,必有一个最小数存在。

证明:分两种情况讨论,即这个集合为有限集或无限集。

(1) 若这个集合为有限集,则根据基数理论或序数理论,任何两个自然数都可比大小,因此一定存在最小数,从而结论成立。

(2) 若这个集合为无限集,设为 N,则对 $\forall m \in N$,从1到 m 共有 m 个自然数,即 N 中不超过 m 的数最多有 m 个。由于 m 是有限数,所以其中必有一个最小数,记为 h。h 对于 N 中不超过 m 的数来说是最小的,而 N 中其余的数都大于 m,因而也大于 h。因此,h 就是 N 中的最小数。

最小数原理对正有理数、正实数并不适用,它是自然数集的一个重要性质,同时也是数学归纳法的理论依据。

运用最小数原理不难得到最大数原理:

定理 1.2 (最大数原理):设 M 是 N 的非空子集,若 M 有上界(即存在一个整数 a,使得对 $\forall m \in M$ 都有 $m \leqslant a$),那么一定存在 $m_0 \in M$,使得对 $\forall m \in M$ 都有 $m \leqslant m_0$,即 m_0 是 M 中的最大自然数。

证明:考虑由所有这样的自然数 t 组成的集合 $T = \{t \mid 对 \forall m \in M, 有 m \leqslant t\}$。由已知条件可得 $a \in T$,说明 T 非空,于是由最小数原理知,集合 T 中有最小数 t_0 存在。

下证 $t_0 \in M$。若 $t_0 \overline{\in} M$,则对任意 $m \in M$,有 $m < t_0$,所以 $m \leqslant t_0 - 1$,这说明 $t_0 - 1 \in T$,这与 t_0 的最小性矛盾。

由 $t_0 \in T$ 且 $t_0 \in M$,从而对 $\forall m \in M$,都有 $m \leqslant t_0$,故取 $t_0 = m_0$,即 m_0 是 M 中最大的自然数。

运用最小数原理还可以证明常用的数学归纳法。

定理 1.3 （数学归纳法原理）：设有一个与自然数 n 有关的命题$P(n)$，如果

(1) 当 $n=1$ 时，$P(n)$成立。

(2) 假设当 $n=k$ 时，$P(n)$成立，则当 $n=k+1$ 时 $P(n)$也成立。

那么对一切自然数 n，$P(n)$成立。

证明：假设 $P(n)$不对一切自然数都成立。令 N 表示使$P(n)$不成立的自然数所组成的集合，则 $N\neq\phi$，根据最小数原理，N 中存在一个最小数h。且 $h\neq 1$（否则与条件(1)矛盾），因此 $h-1$ 是一个自然数。因为 h 是N 中最小的，从而 $h-1\overline{\in} N$，此即 $P(n)$对 $h-1$ 成立；但 $h\in N$ 故$P(n)$对 h 不成立，这与条件(2)矛盾，故 $P(n)$对一切自然数 n 都成立。

例 1 （第二数学归纳法原理）设有一个与自然数 n 有关的命题$P(n)$，如果

(1) 当 $n=1$ 时，$P(n)$成立。

(2) 假设当 $n<k$ 时，$P(n)$成立，则当 $n=k$ 时$P(n)$也成立

那么对一切自然数 n，$P(n)$总成立。

证明 （反证法）：反设定理不成立，并设 T 是$P(n)$不成立的所有自然数组成的集合，T 非空。由最小数原理知集合 T 中必有最小自然数t_0 存在。由于 $P(1)$成立，所以 $t_0>1$，对任意 $n\in N$，当 $n<t_0$ 时，据 T 的定义知必然有$P(n)$成立，由条件(2)知，必有当 $n=t_0$ 时，$P(t_0)$也成立，这说明 $t_0\overline{\in} T$，矛盾。

如果某一命题不是与所有自然数有关的命题，而是与从 k_0 $(k_0>1)$开始的自然数有关，只须把数学归纳原理改为：

(1) 当 $n=k_0$ 时，$P(k_0)$成立。

(2) 假设当 $n=k(k\geqslant k_0)$时，$P(n)$成立，则当 $n=k+1$ 时，$P(n)$也成立。

那么对一切不小于 k_0 的自然数 n，$P(n)$都成立。

例 2 用数学归纳法证明：当 $n \geqslant 2$ 时，

$$\frac{4^n}{n+1} < \frac{(2n)!}{(n!)^2}$$

证明：(1) 当 $n=2$ 时，由于 $\frac{16}{3} < \frac{24}{4}$，故不等式显然成立。

(2) 假设当 $n=k(k \geqslant 2)$ 时，不等式成立，即

$$\frac{4^k}{k+1} < \frac{(2k)!}{(k!)^2}$$

易证 $$4(k+1)^2 < 2(2k+1)(k+2)$$

故 $$0 < \frac{4(k+1)}{k+2} < \frac{2(k+1)(2k+1)}{(k+1)^2}$$

因此 $$\frac{4^k}{k+1} \cdot \frac{4(k+1)}{k+2} < \frac{(2k)!}{(k!)^2} \cdot \frac{2(k+1)(2k+1)}{(k+1)^2}$$

$$= \frac{(2k+2)!}{[(k+1)!]^2}$$

即： $$\frac{4^{k+1}}{k+2} < \frac{(2k+2)!}{[(k+1)!]^2}$$

这说明当 $n=k+1$ 时，不等式也成立。

根据(1)(2)知不等式当 $n \geqslant 2$ 时均成立。

例 3 设有 2^n 个球分成了许多堆，我们可以任意选择甲、乙两堆按以下规则进行挪动：若甲堆的球数 p 不少于乙堆的球数 q，则从甲堆拿 q 个球放至乙堆，称为一次挪动，证明可以经过有限次挪动把所有的球合并成一堆。

证明：(1)当 $n=1$ 时，只有两个球。若这两个球在一堆，则命题成立；若不在一堆，则需挪动一次即可。

(2) 假设 $n=k$ 时，命题成立，即 2^k 个球经过有限次挪动可合并成一堆。现证 $n=k+1$ 时，2^{k+1} 个球的命题也成立。

2^{k+1} 个球分成的各堆球数或奇或偶，而奇数个球的堆数必为偶数，否则总球数将是奇数，现把个数为奇数的堆两两配对，每两堆挪动一次，就会使多堆的球数变为偶数，这样每一堆都变成偶数个球。于是设想把每两个球粘在一起看成一个大球，这时就把

2^{k+1}个球变成了 2^k 个大球，由归纳假设这 2^k 个球可挪成一堆。这就说明 $n=k+1$ 时，命题也成立。

由(1)(2)知，命题对 $\forall n \in N$ 都成立。

1.3 鸽笼原理

鸽笼原理最早来源于这样一个事实：将一群鸽子放入到一些笼子中，已知笼子的数量小于鸽子的数量，则必有一个笼子中有两只或两只以上的鸽子。鸽笼原理最早是由德国数学家狄利克雷明确提出来的，因此又叫狄利克雷原理，也称抽屉原理。

定理 1.4 鸽笼原理：设有 n 个集合 A_1、A_2、$\cdots A_n$，m 个元素 a_1、a_2、$\cdots a_m$，其中 $A_i \cap A_j = \phi (i \neq j)$，$\bigcup_{i=1}^{n} A_i = \{a_1, a_2 \cdots, a_m\}$，则必有一个集合至少含有 k 个元素，其中

$$K = \begin{cases} \dfrac{m}{n} & \dfrac{m}{n}\text{为整数} \\ \left[\dfrac{m}{n}\right]+1 & \dfrac{m}{n}\text{不为整数} \end{cases}$$

其中$\left[\frac{m}{n}\right]$表示为不超过$\frac{m}{n}$的最大整数

用反证法容易得到证明，在此略去。

特别地：当 $m=n+1$ 时，一般称为鸽笼原理Ⅰ：$n+1$ 个物体放入到 n 个抽屉中，则无论怎么放，必有一个抽屉中至少有两件物体。

当 $m=nr+1$ 时，一般称为鸽笼原理Ⅱ：$nr+1$ 个物体放入到 n 个抽屉里，则无论怎么放必有一个抽屉里至少有 $r+1$ 件物体。

例 1 已知整数 $a_1, a_2, \cdots, a_{10}$，求证必存在一个非 0 整数组($x_1, x_2, \cdots, x_n$)，使得对所有的 $x_i \in \{-1,0,1\}$，和式$\sum_{i=1}^{10} x_i a_i$，被 1001 整除。

证明：考虑形如 $g=\sum_{i=1}^{10} x_i a_i$，$x_i \in \{0,1\}$ 的数，这样的数共有 $2^{10}-1=1023>1001$，由鸽笼原理知，必有两个数被 1001 除可得的余数相等，而这两个数的差被 1001 整除，其差仍然形如$\sum_{i=1}^{10} x_i a_i$，

且 $x_i \in \{-1,0,1\}$

例 2　一个旅馆有 90 个房间,住有 100 名旅客,如果每次都恰有 90 名客人同时回来。证明至少要准备 990 把钥匙分给这 100 名客人,才能保证使得每次客人回来时,每个客人都能用自己分到的钥匙打开一个房间住进去;并且避免发生两人住进同一个房间。

证明:如果钥匙数少于 990;则由鸽笼原理知 90 个房间至少有一个房间的钥匙数小于$\frac{990}{90}=11$。当持有这个房间钥匙的客人(至多 10 人)都未回来时,此房间就打不开,这样 90 个人无论如何也不能按所要求的方式在这 89 个房间内住下来。

另外,当钥匙数为 990 时,就可以按所要求的方式住下来,这只须把 90 把不同钥匙分给 90 个人,剩下 10 人每人拿 90 把钥匙(每一个房间一把),那么任何 90 人返回时,都能按要求住进房间。

例 3　任意给定一个 n^2+1 项的实数列,$a_1,a_2,\cdots,a_{n^2+1}$。证明:可以从中选出 $n+1$ 项单调递增或递减的子数列。

证明:在实数列 $a_1,a_2,\cdots,a_{n^2+1}$中,对每一个 a_i,从它开始向右寻找能构成递增子列的那些项,把其中最长的递增子列的长度记为 t_i,则相应地有两个数列。

$a_1,a_2,\cdots,a_{n^2+1}$

$t_1,t_2,\cdots,t_{n^2+1}$

如果已有某个 $t_k \geqslant n+1$,则必可以从 $a_k,a_{k+1},\cdots,a_{n^2+1}$中选出长为 $n+1$ 的递增子列;如果所有的 t_i 均小于 $n+1$,故 t_i 只能至多取值为以下几种情况之一:$1,2,3,\cdots,n$,但共有 n^2+1 个元素 t_i,由鸽笼原理知必有 $n+1$ 个数相同。设这 $n+1$ 个数为 $t_{k_1}=t_{k_2}=\cdots=t_{k_{n+1}}$,其中 $1\leqslant k_1<k_2<\cdots<k_{n+1}\leqslant n^2+1$,其对应的 $a_{k_1},a_{k_2}\cdots,a_{k_{n+1}}$必然满足 $a_{k1}\geqslant a_{k2}\geqslant\cdots\geqslant a_{k_{n+1}}$,否则若当 $k_i<k_j$ 时,有 $a_{ki}<a_{kj}$,则就有 $t_{ki}<t_{kj}$,这与 $t_{ki}=t_{kj}$矛盾。由此可知一定存在 $n+1$ 个元素单调递减子列。

练　习　一

1．由数学归纳法原理推出最小数原理。

2．设 T 是由一些整数组成的集合，若 T 有下界（即存在 $a\in Z$，使得对 $\forall t\in T$，有 $t\geqslant a$），那么必存在 $t_0\in t$，使对所有 $t\in T$，都有 $t\geqslant t_0$。

3．用数学归纳法证明：

(1) 当 $a>0$ 时，$\sqrt{a+\sqrt{a+\sqrt{a+\cdots+\sqrt{a}}}}<\sqrt{a}+1$

(2) x^n+x^{-n} 可展开为 $x+x^{-1}$ 的 n 次多项式

4．设 $f(n)$ 是具有以下性质的函数

(1) $f(n)$ 的定义域是全体自然数

(2) $f(n)$ 是整数

(3) $f(2)=2$

(4) $f(m\cdot n)=f(m)\cdot f(n)$，对一切 m,n 都成立

(5) 当 $m>n$ 时，$f(m)>f(n)$

试用数学归纳法证明 $f(n)=n$

5．设在一个环形公路上有 n 个汽车站，每一站存有汽油若干桶（其中有的站可以不存），n 个站总存油量足够一辆汽车沿此公路行驶一周。现在使一辆原来没油的汽车依逆时针方向沿公路行驶，每到一站即把该站的存油全部带上（出发的站也如此）。试证 n 站之中至少有一站，可以使汽车从此站出发环行一周，不致在中途因缺油而停车。

6．一次象棋比赛共有 n 名选手参加，证明必有两名选手与同样多的对手下过象棋。

7．从整数 1 到 $2n$ 中任取 $n+1$ 个数，求证所取出的 $n+1$ 个数中，一定能找到两个数，它们的差等于 n。

8．15 个人围着一张圆桌坐下，圆桌上预先写好 15 个人的名字，但大家都没注意。坐下后才发现没有一个人与写好的名字相

符。证明可以转动圆桌，使得至少有两个人与他们的名字相符。

9. 在直径为 5 的圆内放入 10 个点，证明其中必有两个点的距离小于 2。

10. 某学生准备用恰好 11 个星期做完数学复习题，每天至少做一道题，每星期至多做 12 道题。证明：一定存在连续的若干天，他恰好做了 21 道题。

11. 6 个代表队共 1958 名运动员，编号为 1，2，…，1958。证明，至少有一名运动员的号码等于他的两名队友的号码的和或一个队友的号码的 2 倍。

12. 平面上任作 8 条直线，互不平行。证明，其中必有两条直线的夹角小于 23°。

§2 整除

2.1 约数和倍数

两个整数的和、差、积仍然是整数，但两整数的商却不一定是整数，因此我们引进整除的概念。

定义 1.10 任意给两个整数 a、b，其中 $b \neq 0$，如果存在整数 q，使得等式 $a = b \cdot q$ 成立，那么就说 b 整除 a，记作 $b \mid a$，此时我们把 b 叫做 a 的约数，把 a 称为 b 的倍数。否则，就说 b 不整除 a，记作 $b \nmid a$。若 $a = qb$，且 $b \neq \pm a$，$b \neq \pm 1$ 则 b 称为 a 的真约数。

简单性质

(1) 1 是任一整数的约数，即 $1 \mid a$。

(2) 0 是任一整数的倍数，即 $b \mid 0$。

(3) 任一非 0 整数是其本身的约数，也是其本身的倍数，即 $a \mid a$。

下面是一些数的整除特征。

(1) 一个整数被 2 整除当且仅当它的个位数字是偶数。

(2) 一个整数被 5 整除当且仅当它的个位数字是 0 或 5。

(3) 一个整数被 3(或 9)整除当且仅当这个整数的各位数字之和是 3(或 9)的倍数。

(4) 一个整数被 4(或 25)整除当且仅当这个整数的末尾两位数是 4(或 25)的倍数。

(5) 整数 $N = \overline{a_n a_{n-1} \cdots a_1}$ 被 7 整除，当且仅当 $\overline{a_n a_{n-1} \cdots a_2} - 2a_1$ 是 7 的倍数。

(6) 整数 $N = \overline{a_n a_{n-1} \cdots a_1}$ 被 11 整除当且仅当 N 的各位数字的交错和 $a_n - a_{n-1} + a_{n-2} + \cdots + (-1)^{n-1} a_1$ 是 11 的倍数。

例 1 设六位数 $\overline{a52bcd}$ 是 3 和 11 的倍数，且它的各位数字之和是 11 的倍数，$b \geqslant d$。求满足此条件的所有的这样的数。

解：由已知 $A = a - 5 + 2 - b + c - d = (a + c) - (b + d) - 3$，$B = (a + c) + (b + d) + 7$ 都是 11 的倍数，故 $A \pm B$ 也是 11 的倍

数，即 $2(a+c)+4$ 和 $2(b+d)+10$ 都是 11 的倍数，又 $1\leqslant a+c\leqslant 18$，故 $6\leqslant 2(a+c)+4\leqslant 40$，由于 $2(a+c)+4$ 是偶数，从而 $2(a+c)+4=22$，即 $a+c=9$，同理可得 $b+d=6$ 或 17

由已知 $3\mid\overline{a52bcd}$ 故 $3\mid(a+c)+(b+d)+7$ 于是 $b+d=17$，又知 $b\geqslant d$ 推出 $b=9,d=8$，而由 $a+c=9$ $(a\neq 0)$ 知 $\begin{cases}a=1\\c=8\end{cases}$ $\begin{cases}a=2\\c=7\end{cases}\cdots\begin{cases}a=9\\c=0\end{cases}$ 故所求的六位数共有九个，分别为 152988，252978，352968，452958，552948，652938，752928，852918，952908。

2.2 基本性质

由整除的定义出发，可得到下列性质：

(1) $b\mid a\Leftrightarrow -b\mid a\Leftrightarrow b\mid -a\Leftrightarrow |b|\mid|a|$

(2) 如果 $b\mid a,c\mid b$，则 $c\mid a$

(3) $c\mid a$ 且 $c\mid b\Leftrightarrow c\mid ma+nb,m,n,\in Z$

(4) 如果 $b\mid a$ 且 $a\neq 0$，则 $|b|\leqslant|a|$，即非零整数仅有有限个因数。

(5) 设 $m\neq 0$，则 $b\mid a\Leftrightarrow mb\mid ma$

(6) $b\mid a$ 且 $a\mid b$，则 $a=\pm b$

(7) 若 $a\mid bc$，且 $(a,c)=1$，则 $a\mid b$

(8) 若 $a\mid b,c\mid b$，且 $(a,c)=1$，则 $a\cdot c\mid b$

例 1 设 n 是正偶数，证明 $2^n-1\nmid 3^n-1$

证明：设 $n=2k$，则 $2^n-1=4^k-1=3M$，其中 M 是正整数，故 $3\mid 2^n-1$。

若 $2^n-1\mid 3^n-1$，则 $3\mid 3^n-1$ 矛盾。因此 $2^n-1\nmid 3^n-1$。

例 2 设 $1\leqslant a_1<a_2<\cdots<a_{n+1}\leqslant 2n$ 则有 $1\leqslant i<j\leqslant n+1$，使得 $a_i\mid a_j$。

证明：令 $a_i=2^{\lambda_i}b_i,\lambda_i\geqslant 0,2\nmid b_i$ 且 $b_i<2n(i=1,2,\cdots\cdots n+1)$，由于 $1,2,\cdots,2n$ 中恰有 n 个不同的奇数。故在 $b_1,b_2,\cdots b_{n+1}$

中必有两个相同，设 $b_i=b_j(1\leqslant i<j\leqslant n+1)$ 故有 $a_i|a_j$。

定理 1.5 设正整数 $n\neq 0$ 有 m 个正约数，设为 $d_1,d_2,d_3,\cdots d_m$，且 $d_1<d_2<\cdots<d_m$，则 $n=d\cdot d_{m+1-k}$，$1\leqslant k\leqslant m$。

证明：n 有 m 个约数 $1<d_1<d_2<\cdots<d_m=n$，由性质知 $\frac{n}{d_i}$ $(1\leqslant i\leqslant m)$ 也是 n 的约数，显然有 $1=\frac{n}{d_m}<\frac{n}{d_{m-1}}<\cdots<\frac{n}{d_1}=n$，又 n 只有 m 个正约数 故

$$\frac{n}{d_m}=d_1,\frac{n}{d_{m-1}}=d_2,\cdots\frac{n}{d_{m+1-k}}=d_k,\cdots\frac{n}{d_1}=d_m$$

$$\therefore\quad n=d_1d_m=d_2d_{m-1}=\cdots=d_kd_{m+1-k}=\cdots=d_md_1$$

即

$$n=d_k\cdot d_{m+1-k}$$

例 3 自然数 N 恰有 12 个正约数，记为 $d_1,d_2,\cdots d_{12}$，且 $d_1<d_2<\cdots<d_{12}$，现知脚标是 d_4-1 的正约数等于乘积 $(d_1+d_2+d_4)d_8$，求 d_4。

解：由定理 1.5 知 $N=d_i\cdot d_{13-i}$，$i=1,2,\cdots 12$ 记 $d_4-1=k$，由已知 $d_k=(d_1+d_2+d_4)\cdot d_8$，可知 $d_1+d_2+d_4$ 是 N 的约数，且 $d_1+d_2+d_4\geqslant d_5$ 这样 $d_k=(d_1+d_2+d_4)\cdot d_8\geqslant d_5\cdot d_8=N$，又 $d_k\leqslant N$

故 $d_k=N$ 即 $k=12$

从而 $d_4-1=12$ 　　于是 $d_4=13$

2.3 数的奇偶性

整数可以分为两大类：奇数和偶数。显然 {偶数} ∩ {奇数} $=\phi$，{偶数} ∪ {奇数} $=Z$

如果用 0 表示偶数，1 表示奇数，有下列加法和乘法运算表

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

例 1 设 $x_1, x_2, \cdots, x_{1997}$都是 1 或者 -1,证明:$x_1+2x_2+3x_3+\cdots+1997x_{1997}\neq 0$

证明:$x_1+2x_2+3x_3+\cdots+1997x_{1997}$

$$\begin{aligned}&=(x_1+|x_1|)+2(x_2+|x_2|)+3(x_3+|x_3|)+\cdots+1997(x_{1997}+|x_{1997}|)-(|x_1|+2|x_2|+3|x_3|+\cdots+1997|x_{1997}|)\\&=(x_1+|x_1|)+2(x_2+|x_2|)+\cdots+1997(x_{1997}+|x_{1997}|)-(1+2+3+\cdots+1997)\\&=(x_1+|x_1|)+2(x_2+|x_2|)+\cdots+1997(x_{1997}+|x_{1997}|)-999\times1997\end{aligned}$$

由于 $x_i\in\{-1,1\}$,所以$(x_i+|x_i|)\in\{0,2\}$,即$[x_1+|x_1|+2(x_2+|x_2|)+\cdots+1997(x_{1997}+|x_{1997}|)]$是偶数,而 199×1997 是奇数,故有

$x_1+2x_2+3x_3+\cdots+1997x_{1997}\neq 0$

例 2 设数列 1,9,8,3,4,3,…其中 a_{n+4}为 a_n+a_{n+3}的个位数字($n=1,2,3,\cdots$),试证 $a_{1998}^2+a_{1999}^2+a_{2000}^2+3$ 是 4 的倍数。

证明:将原数列中 a_n 的奇偶性分别用 1、0 代替,则可得数列 $\{b_n\}$:1,1,0,1,0,1,1,0,0,1,0,0,0,1,1,……显然有下列两个结论:

(1) a_n 与 b_n 的奇偶性相同

(2) $b_n=b_{(n+15t)}$(t 是任意的正整数)

而 $2000=133\times15+5$ $\therefore b_{2000}=0, b_{1999}=1$ $b_{1998}=0$。这说明 a_{1998}和 a_{2000}为偶数,而 a_{1999}为奇数。从而

$a_{1998}^2+a_{1999}^2+a_{2000}^2+3$ 是 4 的倍数。

例 3 坐标平面上有一条封闭折线 $A_1,A_2,A_3,\cdots A_nA_1$,它们的所有顶点 $A_i(i=1,2,\cdots,n)$都是格点(即横、纵坐标都是整数的点),且$|A_1A_2|=|A_2A_3|=\cdots=|A_{n-1}A_n|=|A_nA_1|$。证明:$n$ 不可能是奇数。

证明:设 $A_i(x_i, y_i)(i=1,2,\cdots,n)$其中 $x_i, y_i \in Z$,因为 $|A_1A_2| = |A_2A_3| = \cdots = |A_nA_1|$

即 $(x_1-x_2)^2+(y_1-y_2)^2=(x_2-x_3)^2+(y_2-y_3)^2=\cdots$
$\cdots=(x_{n-1}-x_n)^2+(y_{n-1}-y_n)^2=(x_n-x_1)^2+(y_n-y_1)^2$

设 $\alpha_1=x_1-x_2, \alpha_2=x_2-x_3, \cdots \alpha_{n-1}=x_{n-1}-x_n, \alpha_n=x_n-x_1$
$\beta_1=y_1-y_2, \beta_2=y_2-y_3, \cdots \beta_{n-1}=y_{n-1}-y_n, \beta_n=y_n-y_1$

则 $\alpha_1^2+\beta_1^2=\alpha_2^2+\beta_2^2=\cdots=\alpha_n^2+\beta_n^2=M$ …………(1)

因为 $A_1A_2\cdots A_nA_1$ 是封闭折线

所以 $\alpha_1+\alpha_2+\cdots+\alpha_n=0$………(2)

$\beta_1+\beta_2+\cdots+\beta_n=0$……(3)

又因为 $x_i, y_i \in Z$,所以 $\alpha_i, \beta_i \in Z$

若所有的 α_i, β_i 均为偶数,总可以用 2^T 去除所有的 $\alpha_i\beta_i$,设 $\alpha_i'=\frac{\alpha_i}{2^T}, \beta_i'=\frac{\beta_i}{2^T}$,则在所有的 α_i'和β_i'中必有一个是奇数,且上述(1)(2)(3)式可化为:$\alpha_1'^2+\beta_1'^2=\alpha_2'^2+\beta_2'^2=\cdots=\alpha_n'^2+\beta_n'^2=M'$不妨设$\alpha_1'+\alpha_2'+\cdots+\alpha_n'=0, \beta_1'+\beta_2'+\cdots+\beta_n'=0$,为方便起见,仍用 α_i, β_i 表示,α_1 是奇数。

(1) 当 β_1 是偶数时

设 $\alpha_1=2m+1, \beta_1=2m', m_1m' \in Z$

则 $\alpha_1^2+\beta_1^2=(2m+1)^2+4m'^2=4(m^2+m+m'^2)+1$

令 $k=m^2+m+m'^2$,则 $k\in Z, \alpha_1^2+\beta_1^2=4k+1$

又 $\alpha_1^2+\beta_1^2=M$,所以 $M=4k+1$

由(1)式得 $\alpha_i^2+\beta_i^2=4k+1(i=1,2\cdots n)$

$\therefore \alpha_i$ 与β_i 必为一奇一偶。所以在 $\alpha_1, \alpha_2\cdots\alpha_n, \beta_1, \beta_2\cdots\beta_n$ 中必有n 个奇数n 个偶数,由(2)和(3)可得:$\alpha_1+\alpha_2+\cdots+\alpha_n+\beta_1+\beta_2+\cdots+\beta_n=0$

即 n 个偶数 + n 个奇数之和 = 0

所以 n 个奇数之和必为偶数，

所以 n 必为偶数。

(2) 当 β_1 为奇数时

$\because \alpha_1{}^2+\beta_1{}^2=M \qquad \therefore M=4k+2$

$\therefore \alpha_i$ 与 β_i 必同为奇数，$i=1,2\cdots n$

由(2)式得 $\alpha_1+\alpha_2+\cdots+\alpha_n=0$

所以 n 为偶数

综上所述，n 不可能为奇数。

例 4 能否把 1、1、2、2、3、3…1986，1986 这 3972 个数字排成一行，使得两个 1 之间夹 1 个数，两个 2 之间夹两个数……两个 1986 之间夹 1986 个数。证明你的结论。

解：假设能按题目要求排出一行数，所有这些数将占有 3972 个位置，把每个位置以 1，2，3…3972 编上 3972 个号码，当 $i=1,2,3,\cdots 1986$ 时，每个 i 将占有两个不同的位置，将这两个位置的序号分别记为 $a_i, b_i(1\leqslant a_i<b_i\leqslant 3972)$

由题意有 $b_i-a_i=i+1$

$\therefore a_i+b_i=2a_i+i+1=$ 偶数 $+i+1$

将这 1986 个等式相加得：

$1+2+3+\cdots+3972=$ 偶数 $+(1+2+3+\cdots 1986)+1986$

即 $$\frac{3972\times 3973}{2}=\text{偶数}+\frac{1986\times 1987}{2}$$

整理得 $1986\times 3973=$ 偶数 $+993\times 1987$

而左端是偶数，右端是奇数这显然是不可能成立的

故题目所要求的排法不存在。

练　习　二

1. 已知存在正整数 n,使 $1987 \mid \underbrace{11\cdots1}_{n个}$,证明 $1987 \mid \underbrace{11\cdots1}_{n+1个}\underbrace{99\cdots9}_{n+1个}\underbrace{88\cdots8}_{n+1个}\underbrace{77\cdots7}_{n+1个}$

2. 用 1,2,3,4,5,6 组成一个六位数$\overline{abcdef}$,其中不同的字母代表不同的数字。要求 $2\mid\overline{ab}$,$3\mid\overline{abc}$,$4\mid\overline{abcd}$,$5\mid\overline{abcde}$,$6\mid\overline{abcdef}$,求此六位数$\overline{abcdef}$

3. 已知八位数$\overline{141x24y3}$是 99 的倍数,求 x、y。

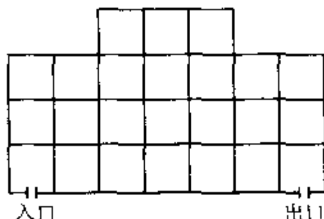
4. 若 $x_1, x_2 \in \{-1,1\}$　且 $x_1x_2 + x_2x_3 + \cdots + x_nx_1 = 0$　则 $4\mid n$

5. 在一条环形公路上,n 个车站被 n 段公路连接起来,车站所在地的高度有海拔 50 米和 100 米两种。相邻两车站若海拔高度相同,则它们之间的一段公路是水平的。否则是上坡路或下坡路。有一个乘客乘汽车在这条环形公路上沿逆时针方向兜了一圈,发现有坡公路的段数与水平公路的段数一样多,求证:$4\mid n$

6. 有 $n\times n(n\geqslant4)$的一张空白方格表,在它的每一个方格内任意地填入 +1 和 −1 中的某一个。现将表内几个两两既不同行又不同列的方格中的数的乘积称为一个基本项。试证:按上述方式所填成的每一个方格表,它的全部基本项之和总能被 4 整除。

7. 桌上有 7 只茶杯,杯口全部朝上,每次"操作"是指将其中 4 只杯子同时翻转,问能否经过若干次运动使杯口全部朝下?

8. 一个展览厅,如图所示。共 24 间展室,其中任何两个相邻的展室之间都有门相通。问能否设计出从入口到出口的参观路线,不重不漏的走过每间展室?



§3 素数与合数

3.1 素数与合数概念

依据一个数的正因数的个数,可将所有的正整数分为三类:

(1) 只有一个正因数的正整数,显然这种数只有一个,就是1。

(2) 恰有两个正因数的正整数,这两个正因数就是1和它自身,如2,3,5,7,…

(3) 至少有三个正因数的正整数,如4,6,8…,显然这种数至少有一个真因数。

定义1.11 大于1且只有1和其自身这两个正因数的正整数称为素数(也称质数或不可约数);大于1而不是素数的正整数,称为合数(也称复合数)。

由定义1.11知,1既不是素数也不是合数;2是唯一的偶素数。

例1 n 是一确定的非负整数,且 $2n+1$ 和 $3n+1$ 是完全平方数,问 $5n+1$ 是素数吗?

解:设 $2n+1=k^2,3n+1=m^2,k,m\in N$

则 $5n+1=4(2n+1)-(3n+1)=4k^2-m^2=(2k+m)(2k-m)$

其中 $2k-m\neq 1$,否则 $2k-m=1$,则有 $5n+3=2m+1$,于是 $(m-1)^2=m^2-(2m+1)+2=(3n+1)-(5n+3)+2=-2n<0$,矛盾

这说明 $2k-m\neq 1$,显然 $2k+m\neq 1$,于是 $5n+3$ 不是素数。

例2 一个整数有四个质因数,如果这四个质因子的平方和是467,求此数。

注:质因数即素因数,指如果一个整数的除数是不可约数(即素数),那么这个除数就称为素因数或素约数

解:设 $p\neq 3$ 是素数,则 p 必是下列形式之一:$3k+1,3k+2$,从而 $p^2=3m+1$

又 $467=158\times3+2$

这说明 467 有两个非 3 的素因数，记为 p、q，则另两个素因数均为 3，这样就有

$$p^2+q^2=476-2\times3^2=458<22^2=484$$

不妨谈 $p>q$，则 $16<p<21$

当 $p=17$ 时，$q=13$

当 $p=19$ 时，无解

因此这个整数的四个素因子为 3,3,17,13 故所求的整数为 $3^2\times17\times13-1989$。

例 3 试证存在无穷多个自然数 n，使得 $z=n^4+a$ 均为合数。

证明：取 $a=4m^4$，m 是大于 1 的整数。

$$
\begin{aligned}
\text{则 } n^4+a &= n^4+4m^4=(n^2+2m^2)^2-4n^2m^2\\
&=(n^2+2m^2-2nm)(n^2+2m^2+2nm)\\
&=[(n+m)^2+m^2]\cdot[(m-n)^2+m^2]
\end{aligned}
$$

因为，$m>1$

所以，上式两个因式均大于 1

故 z 必为合数，又 m 为任意的大于 1 的整数，则 $a=4m^4$ 也有无穷多个，即原结论成立。

3.2 性质

由素数与合数的定义易得

定理 1.6 （ⅰ）$a(a>1)$是合数的充要条件是 $a=de$，$1<d$，$e<a$。

（ⅱ）若 $d>1$，q 是素数，且 $d\mid q$ 则 $d=q$

定理 1.7 若 a 是合数，则必有素数 $p\mid a$

证明：由定理 1.6 知 a 必有约数 $d\geqslant2$，设集合 T 由 a 的所有约数（$d\geqslant2$）组成，由最小数原理知集合 T 中必有最小数存在，设为 p。则 p 一定是素数。否则 $p\geqslant2$ 是合数，则 p 必有约数 d'，$2\leqslant d'<p$，显然 $d'\in T$，这与 p 的最小性矛盾。从而原命题成立。

定理 1.8 设整数 $a \geqslant 2$,那么,a 一定可表为素数的乘积,即 $a = p_1 p_2 \cdots p_s$,其中 $p_i(1 \leqslant i \leqslant s)$是素数。

证明(用第二数学归纳法),当 $a = 2$ 时,2 是素数,从而结论成立,假设对某个 $n > 2$,当 $2 \leqslant a < n$ 时,结论对所有这种 a 都成立。则当 $a = n$ 时,若 n 是素数,则结论成立;若 n 是合数,则必有 $n = n_1 n_2, 2 \leqslant n_1, n_2 < n$。由假设 n_1, n_2 均可表示为素数之积;

$$n_1 = p_{11} \cdot p_{12} \cdots\cdots p_{1s}, n_2 = p_{21} \cdot p_{22} \cdots\cdots p_{2r}$$

这样,就把 a 表为素数的乘积

$$a = n = n_1 n_2 = p_{11} \cdot p_{12} \cdots p_{1s} \cdot p_{21} \cdot p_{22} \cdots p_{2r}$$

因此,由第二数学归纳法,定理对所有 $a \geqslant 2$ 都成立。

例如,1260 的不同素因数有 2,3,5,7 四个,这样就有 $1260 = 2^2 \cdot 3^2 \cdot 5 \cdot 7$

由定理 1.8 容易推出:

推论:设整数 $a \geqslant 2$

(ⅰ) 若 a 是合数,则必有素数 $p \mid a, p \leqslant \sqrt{a}$

(ⅱ) 若 $a = p_1 p_2 \cdots\cdots p_s$,则必有素数 $p \mid a, p \leqslant \sqrt[s]{a}$

例如当 $a = 1260 = 2 \times 2 \times 3 \times 3 \times 5 \times 7$ 时,$s = 6$,它的素因数 2 就满足 $2 < \sqrt[6]{1260} \approx 3.28$

定理 1.9 素数全体构成的集合是无限集。

证明(反证法),假设全体素数是有限个,不妨设 $Q = \{q_1, q_2, \cdots q_k\}$是全体素数的集合,考虑 $a = q_1 \cdot q_2 \cdots q_k + 1$,显然 $a > 2$,由定理 1.7 知必有素数 $p \mid a$,由假设 p 等于某个 q_i,因而 $p \mid 1$ 矛盾,因此全体素数集合必是无限集。

设 $q_1 = 2, q_2 = 3, q_3 = 5, q_4, q_5, \cdots$是全体素数按从小到大顺序排列,以及

$$Q_k = q_1 q_2 \cdots q_k + 1$$

直接计算得 $Q_1 = 3, Q_2 = 7, Q_3 = 31, Q_4 = 211, Q_5 = 2311, Q_6 = 59 \cdot 509, Q_7 = 19 \cdot 97 \cdot 277, Q_8 = 347 \cdot 27953, Q_9 = 317 \cdot 703763, Q_{10} = 331 \cdot 571 \cdot 34231$

这里前 5 个数是素数，后 5 个数是合数，但 Q_k 都有一个比 q_k 更大的素数，至今还不知道是否存在无穷多个 k 使 Q_k 是素数，也不知道是否有无穷多个 k 使 Q_k 是合数。

定理 1.9 是数论中一个非常重要的定理，由它的证明可以得到不超过 x 的素数个数——记为 $\pi(x)$的一个很弱的下界估计，及第 n 个素数 p_n 大小的一个很弱的上界估计。

定理 1.10 设全体素数按从小到大排列的序列是 $p_1=2, p_2=3, p_3, p_4, \cdots$则有 $p_n \leqslant 2^{2^{n-1}}$ $n=1,2,\cdots$及 $\pi(x)>\log_2\log_2 x, x\geqslant 2$

证明：由定理 1.9 的证明知

$$p_n \leqslant p_1 p_2 \cdots p_{n-1}+1, n>1 \qquad (1)$$

现用数学归纳法来证明结论 $p_n \leqslant 2^{2^{n-1}}$

当 $n=1$ 时，$p_1 \leqslant 2$ 显然成立，假设 $n \leqslant k(\geqslant 1)$时成立，当 $n=k+1$ 时，由式(1)及归纳假设得

$$p_{k+1} \leqslant p_1 p_2 \cdots p_{k-1} p_k+1 \leqslant 2^{2^0} \cdot 2^{2^1} \cdots 2^{2^{k-1}}+1=2^{2^k-1}+1<2^{2^k}$$

这说明命题对 $n=k+1$ 时也成立，从而对任意 n 都成立。

下面来证明 $\pi(x)>\log_2\log_2 x, x\geqslant 2$

对于 $x\geqslant 2$，必有唯一的正整数 n，使得 $2^{2^{n-1}} \leqslant x<2^{2^n}$，因而有 $\pi(x) \geqslant \pi(2^{2^{n-1}}) \geqslant n$

而由 $x<2^{2^n}$得 $\log_2 x<\log_2 2^{2^n}=2^n$

从而 $\log_2\log_2 x<n$

故得 $\pi(x) \geqslant n>\log_2\log_2 x \quad n\geqslant 2$

此外定理 1.9 还表明对于任给的自然数 n，都有大于 n 的素数，这样就产生了寻找大素数的问题。为此，人们研究了用多项式能否表达素数的问题。

定理 1.11 设 a_0 是整数，$a_1, a_2, \cdots a_n$ 是不全为 0 的整数，$f(x)=a_0+a_1 x+\cdots+a_n x^n$，则对任意整数 x，$f(x)$的值不全是素数。

证明:假设对任意整数 x, $f(x)$恒为素数,于是存在整数 a 及素数 $p>2$,使得 $f(a)=p$, $(x-a)|(f(x)-f(a))$。取 $x=a+tp$, $t\in Z$,易知 $p|f(a+tp)-f(a)$

而 $f(a+tp)-f(a)=f(a+tp)-p$

∴ $p|f(a+tp)$

又注意到方程$|f(a+tp)|=p$ 关于 t 至多有 $2n$ 个解,故有整数 t_0,使得$|f(a+t_0p)|=mp$, $m\in Z$, $m>1$,因此 $f(a+t_0p)$是合数,这与 $f(x)$恒为素数矛盾。

此定理表明不存在对任意整数恒取素数的整系数多项式,但是人们却发现了当 $0\leqslant n<17$ 时, n^2-n+17 均为素数;当 $0\leqslant n\leqslant 41$ 时, n^2-n+41 均为素数,那么对任意整数 n,可否求出一个素数 p,使当 $0\leqslant n<p$, n^2-n+p 均为素数,这个问题至今尚未解决。

下面我们考虑形如 $F_n=2^{2^n}+1$ 的数,这种数称为(费尔马)(Fermat)数,前 5 个 Fermat 数都是素数, $F_0=3$, $F_1=5$, $F_2=17$, $F_3=257$, $F_4=65537$,据此,Fermat 曾猜想所有的 F_n 都是素数,但是不久,欧拉(Enler)证明了 F_5 是合数,从而否定了费尔马的这一猜想。

例 1 证明 F_5 是合数

证明:设 $a=2^7$, $b=5$,则 $a-b^3=3$, $1+ab-b^4=1+3b=2^4$ 这样有:

$$F_5=2^{2^5}+1=(2a)^4+1=(1+ab-b^4)a^4+1$$
$$=(1+ab)a^4+1-a^4b^4$$
$$=(1+ab)(a^4+(1-ab)(1+a^2b^2))$$

$1+ab=641$ 故 $641\ |F_5$

即 $F_5=641\times 6700417$

至今, F_0、F_1、F_2、F_3、F_4 是人们所知的费尔马数中仅有的素数。

3.3 逐步淘汰原则

逐步淘汰原则又叫容斥原理，它是组合数学中的一个基本计数理论，正确熟练地使用此原理，可以解决数学竞赛中许多有趣的问题。

考虑一个具有几个元素数的集合 S，其中各元素数往往具有不同的性质，现假设共有 r 种性质记为 $P_1, P_2, \cdots Pr$，组成性质集合 P，即

$P = \{P_1, P_2, P_3, \cdots, Pr\}$

令 A_i 表示 S 中具有性质 Pi 的元素的子集，其元素数个数记为 $n(P_i)$；$A_1 \cap A_2$ 表示 S 中同时具有性质 P_1 和 P_2 的元素的子集，其元素的个数记为 $n(P_1, P_2)$；$\overline{A}_1 \cap \overline{A}_2$ 表示 S 中不具有 P_1 也不具有性质 P_2 的元素数的子集其元素的个数记为 $n(\overline{P_1}, \overline{P}_2)$。

定理 1.12 （逐步淘汰原理）

$$n(\overline{P}_1, \overline{P}_2, \cdots \overline{P}r) = |S| - \sum_{i=1}^{r} n(Pi) + \sum_{i_1 < i_2} n(Pi_1, Pi_2) - \sum_{i_1 < i_2 < i_3} n(Pi_1, Pi_2, Pi_3) + \cdots + (-1)^r \cdot n(P_1, P_2, \cdots P_r)$$

证明：定理的关键是要证明：对不具有 r 个性质中任何一个性质的元素，在此公式中都准确的被计数过一次，而对于至少具有性质之一的元素，在公式中计数为 0 次。

首先计某一元素 $a \in S$，且 a 不具有任何一种性质，它在 $|S|$ 中计数为 1 次而在其余各项计数为 0，故它在公式中总计数为 1。

其次考虑某一元素 $b \in S$，且 b 恰好具有 k 个性质（$1 \leqslant k \leqslant r$）。$b$ 在 s 中被计数次数为 1 即为 $\binom{k}{0}$；在 $\sum n(Pi)$ 中一共被计数了 $\binom{k}{1}$ 次，在 $\sum n(Pi_1, Pi_2)$ 中，它被计数了 $\binom{k}{2}$ 次，在 $\sum n(Pi_1, Pi_2, Pi_3)$ 中，它被计数了 $\binom{k}{3}$ 次，依次类推，元素在公式中被计次数总和为

$\binom{k}{0}-\binom{k}{1}+\binom{k}{2}-\cdots+(-1)^r\binom{k}{r}=(1-1)^k=0$ 其中当 $r>k$ 时，$\binom{k}{r}=0$，由此可知，当元素 b 至少具有这些性质之一时，它在公式中的计数为 0，综合以上讨论，定理得证。

推论，集合 S 中至少具有性质 $P_1, P_2, \cdots, Pr$ 中的一个性质的元素个数为

$$
\begin{aligned}
|A_1 \cup A_2 \cup \cdots \cup Ar| = \sum_{i=1}^{r} n(p_i) - \sum_{i_1<i_2} n(p_{i1}, p_{i2}) \\
+ \sum_{i_1<i_2<i_3} n(p_{i1}, p_{i2}, p_{i3}) - \cdots \\
+ (-1)^{r+1} n(p_1, p_2, \cdots, p_r)
\end{aligned}
$$

推论的证明可由 $|A_1 \cup A_2 \cup \cdots \cup Ar| = |S| - n(\overline{p}_1, \overline{p}_2, \cdots, \overline{p_r})$ 容易得到。

例 1 来自不同国家的 n 个代表参加圆桌会议讨论共同关心的问题。如果 A、B、C 三国的代表座位不能相邻。问座位的安排方式有几种？

解：设性质 P_1 表示 A 与 B 邻，P_2 表示 A 与 C 相邻，P_3 表示 B 与 C 相邻。把座位号依次编为 $1, 2, \cdots, N$，N 号位与 1 号相邻。

全体排列共有 $(n-1)!$ 种，$n(Pi)=2\cdot(n-2)!$ $i=1,2,3$，P_1, P_2, P_3，$n(Pi, P_j)=2\cdot(n-3)!$ $(i\neq j, i, j=1,2,3)$，$n(p_1, p_2, p_3)=0$

于是 $n(\overline{p}_1, \overline{p}_2, \overline{p}_3)=(n-1)! -3\cdot2\cdot(n-2)! +3\cdot2\cdot(n-3)!$
$\quad\quad = (n-3)! \cdot(n-4)\cdot(n-5) \quad n>5$

当 $n\leqslant5$ 时，实际操作可知，不能安排。

下面研究另一个性质，假设集合 s 具有 n 个元素，性质集合记为 $p=\{p_1, p_2, \cdots, p_r\}$，如果要求这 n 个元素中恰好具有 m 个性质 $(1\leqslant m\leqslant r)$ 的元素的个数，则下面定理成立：

定理 1.13 令 $N[m]$ 表示集合 s 中恰好具有 m 个性质的元素个数，则

$$N[m]=\sum n(p_{i1},p_{i2},\cdots,p_{im})-\binom{m+1}{m}\sum n(p_{i1},\cdots,p_{im+1})+\cdots+(-1)^{k-m}\binom{k}{m}\sum n(p_{i1},\cdots p_{ik})+(-1)^{k-m}\binom{r}{m}n(p_1,p_2,\cdots,p_r)$$

证明:同定理 1.12 的证明类似,从等式可以看出,在右端的和式中,对于每个具有小于 m 个性质的元素没有计入。对于每个恰好具有 m 个性质的元素,在和式$\sum n(p_{i1},p_{i2},\cdots,p_{im})$中均被计算了一次。

对于每个具有 k 个性质($k>m$)的特定元素 a,我们只要证明均被算了零次就可以了。由公式可以推得这种 a 在和式中被计数的总次数为:

$$\binom{k}{m}-\binom{k}{m+1}\binom{m+1}{m}+\binom{k}{m+2}\binom{m+2}{m}-\cdots+(-1)^{k-m}\binom{k}{k}\binom{k}{m}$$

$$=\binom{k}{m}\left[\binom{k-m}{k-m}-\binom{k-m}{k-(m+1)}+\binom{k-m}{k-(m+2)}-\cdots+(-1)^{k-m}\binom{k-m}{k-k}\right]$$

$$=\binom{k}{m}\left[\binom{k-m}{0}-\binom{k-m}{1}+\binom{k-m}{2}-\cdots+(-1)^{k-m}\binom{k-m}{k-m}\right]$$

$$=\binom{k}{m}(1-1)^{k-m}=0$$

其中计算中利用了公式

$$\binom{k}{t}\binom{t}{m}=\binom{k}{m}\binom{k-m}{k-t}\quad(m\leqslant t\leqslant k)$$

以上等式说明:当 $k>m$ 时,元素 a 若具有 k 个性质,则等式右端对它的计数为 0,定理证毕。

例 2 (错位问题)将 1,2,$\cdots n$ 重新排列。

(1) 求恰有 $m(m\leqslant n)$个数在其自身位置的排列个数(记作 $Dn[m]$)。

(2) 求没有在其自身位置的排列的总个数,即错位排列数 Dn。

解:设 Pi 表示在排列中数 i 在其自身位置,故 $n(Pi)=(n-1)!$ $(i=1,2\cdots n)$ $n(p_{i1},p_{i2},\cdots p_{ik})=(n-k)!$

故知 $\sum_{1\leqslant i1<i2<\cdots<ik\leqslant n} n(p_{i1},p_{i2}\cdots p_{ik})=\binom{n}{k}(n-k)!$

$\therefore Dn[m]=\binom{n}{m}(n-m)! - \binom{m+1}{m}\binom{n}{m+1}[n-(m+1)]!$

$+\binom{m+2}{m}\binom{n}{m+2}[n-(m+2)]! - \cdots + (-1)^{n-m}\binom{n}{m}$

$= \frac{n!}{m!} - \frac{(m+1)!}{m!\cdot 1!}\cdot\frac{n!}{(m+1)!} + \cdots + (-1)^{n-m}$

$\frac{n!}{(n-m)!\ m!}\cdot\frac{n!}{n!}$

$=\frac{n!}{m!}\left(\frac{1}{2!}-\frac{1}{3!}+\frac{1}{4!}-\cdots+(-1)^{n-m}\cdot\frac{1}{(n-m)!}\right)$

当 $m=0$ 时,问题(2)的解即可得到

$Dn=n!\ \left(1-\frac{1}{1!}+\frac{1}{2!}-\cdots+(-1)^{n}\cdot\frac{1}{n!}\right)$

例 3 在 1 至 120 的自然数中,不能被 2、3、5、7 中某一个数整除的整数有多少个?

解:设 P_1,P_2,P_3,P_4 分别表示能被 2,3,5,7 整除,则

$n(p_1)-60,n(p_2)=\frac{120}{3}=40,n(p_3)=\frac{120}{5}=24,n(p_4)-\left[\frac{120}{7}\right]=17,n(p_1,p_2)=\frac{120}{2\times 3}=20$

$n(p_1,p_3)=\frac{120}{2\times 5}=120,n(p_1,p_4)=\left[\frac{120}{2\times 7}\right]=8$

$n(p_2\ p_3)=\frac{120}{3\times 5}=8,\ n(p_2\ p_4)=\left[\frac{120}{3\times 7}\right]=5$

$n(p_3,p_4)=\frac{120}{5\times 7}=3,n(p_1\ p_2\ p_3)=\frac{120}{2\times 3\times 5}=4$

$n(p_2,p_3,p_4)=\left[\frac{120}{3\times 5\times 7}\right]=1,n(p_1\ p_2\ p_4)=\left[\frac{120}{2\times 3\times 7}\right]=2$

$n(p_1\ p_3\ p_4)=\left[\frac{120}{2\times 5\times 7}\right]=1,n(p_1,p_2,p_3,p_4)=0$

从而 $n(\bar{p}_1,\bar{p}_2,\bar{p}_3,\bar{p}_4)$

$=120-(60+40+24+17)+(20+12+8+8+5+3)$

$$-(4+2+1+1)+0$$
$$=27$$

现在我们来研究不超过 N 的所有素数,并计算出素数的个数。

由定理 1.8 的推论(1)知,只要先求出不超过$\sqrt{N}$的全部素数,$p_1,p_2,\cdots,p_s$ 即可。例如取 N 为 100,不超过 10 的全部素数为 2,3,5,7,依次把不超过 100 的正整数中除了 2,3,5,7(或 $p_1,\cdots,p_s$)以外的 2 的倍数、3 的倍数、5 的倍数、7 的倍数(或 p_1 的倍数,…,p_s 的倍数)全部删去,就删去了不超过 100 的全部合数,剩下的正好就是不超过 100 的全部素数。具体做法见下表,取 $N=100$

1	2	3	4	5	6	7	8	9	10	11	12
13	14	15	16	17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32	33	34	35	36
37	38	39	40	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72
73	74	75	76	77	78	79	80	81	82	83	84
85	86	87	88	89	90	91	92	93	94	95	96
97	98	99	100								

由上表可以看出,没有删去的数是 2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97 共有 25 个,它们就是不超过 100 的全部素数。从这不超过 100 的 25 个素数出发,重复上面做法,就可找出不超过 $100^2=10000$ 的全部素数。这种寻找素数的方法,通常叫做爱拉托斯芬(Eratoschenes)筛法。

下面我们来求通过爱拉托斯分(Eratoschenes)筛法后剩下的素数的个数。

令 $\pi(x)$表示区间$[2,x]$上素数的个数,$\sqrt{n}$至 n 的素数的个数应为 $\pi(n)-\pi(\sqrt{n})$,它又是$[2,n]$中不能被$\{p_1,p_2,\cdots,p_s\}$中任一数整除的个数,仿照例 1,就可得到下面的计算素数个数的公式:

$$\pi(n)-\pi(\sqrt{n})=n-1-\sum_{i=1}^{n}\left[\frac{n}{p_i}\right]+\sum_{i_1<i_2}\left[\frac{n}{p_{i1}p_{i2}}\right]$$
$$-\cdots+(-1)^s\cdot\left[\frac{n}{p_1p_2\cdots p_s}\right]$$

在 1~1000 中间有 168 个素数

在 1001~2000 中有 135 个素数

在 2001~3000 中有 127 个素数

在 3001~4000 中有 120 个素数

一般地,有下面定理。

定理 1.14 (素数分布)设 $\pi(x)$表示 $1,2,\cdots,[x]$中的素数个数,例如:$\pi(3)=2,\pi(5.1)=3$,

$\pi(\sqrt{85})=4,\cdots$则 $\lim\limits_{x\to+\infty}\frac{\pi(x)}{x}=0$

特别地 $\lim\limits_{n\to+\infty}\frac{\pi(n)}{n}=0$

这表明前 n 个自然数中素数个数与 n 的比值接近于 0,也即几乎所有整数都是合数。

证明:用 S 表示 $1,2,\cdots,[x]$所组成的自然数集合,显然$|S|=[x]$,以 $P_1=2<P_2<\cdots<Pr$ 表示前 r 个素数,用 $Ai(1\leqslant i\leqslant r)$表示 S 中能被素数$Pi(1\leqslant i\leqslant r)$整除的自然数个数。我们首先求 S 中不能被 $P_1,P_2,\cdots,Pr$ 中任一素数所整除的自然数。于是由逐步淘汰原理有:

$$|\overline{A}_1\cap\overline{A}_2\cap\cdots\cap\overline{A}r|=|s|-\sum\cap Ai|+\sum|Ai\cap Aj|-\cdots+$$
$$+(-1)^r|A_1\cap A_2\cap\cdots\cap Ar|$$

$$=[x]-\sum_{1\leqslant i\leqslant r}\left[\frac{x}{Pi}\right]+\sum_{1\leqslant i<j\leqslant r}\left[\frac{x}{PiPj}\right]-\cdots$$

$$-(-1)^r\left[\frac{x}{p_1p_2\cdots p_r}\right] \qquad \cdots(1)$$

容易看出,S 中每个素数(除去含在 $p_1,p_2,\cdots,p_r$ 以外)都不能被 $p_1,\cdots,p_r$ 中任一个素数整除,而反过来,S 中不能被 $p_1,\cdots,p_r$ 中任一素数整除的数未必就是一个素数,因此我们有

$$\pi(x)\leqslant|\overline{A}_1\cap\overline{A}_2\cap\cdots\cap\overline{A}_r|+r \qquad \cdots \quad (2)$$

利用不等式 $y-1<[y]<y+1$ 及(1)(2)式得

$$\pi(x)<(x+1)-\sum_{1\leqslant i\leqslant r}\left(\frac{x}{p_i}-1\right)+\sum_{1\leqslant i<j\leqslant r}\left(\frac{x}{p_ip_j}+1\right)-\cdots$$

$$+(-1)^r\left(\frac{x}{p_1p_2\cdots p_r}+(-1)^r\right)+r$$

$$=x\left(1-\frac{1}{P_1}\right)\cdots\left(1-\frac{1}{P_r}\right)+\left(1+\binom{r}{1}+\cdots+\binom{r}{r}\right)+r$$

$$=x\cdot\prod_{i=1}^{r}\left(1-\frac{1}{P_i}\right)+2^r+r \qquad \cdots(3)$$

容易看出有 $\prod_{P\leqslant P_r}\left(1-\frac{1}{P}\right)^{-1}=\prod_{P\leqslant P_r}\left(1+\frac{1}{P}+\frac{1}{P^2}+\cdots\right)$

对每个 $Pj(1\leqslant j\leqslant r)$,取 Sj 为满足 $P_j^{sj}\geqslant Pr$ 的最小自然数,则有(显然 $Sr=1$)

$$\prod_{P\leqslant Pr}\left(1-\frac{1}{P}\right)^{-1}\geqslant\left(1+\frac{1}{P_1}+\cdots+\frac{1}{{P_1}^{s_1}}\right)\left(1+\frac{1}{P_2}+\cdots+\frac{1}{{P_2}^{s_2}}\right)\cdots$$

$$\left(1+\frac{1}{P_{r-1}}+\cdots+\frac{1}{P_{r-1}^{Sr-1}}\right)\left(1+\frac{1}{p_r}\right)$$

$$\geqslant1+\frac{1}{2}+\cdots+\frac{1}{Pr}$$

$$>1+\frac{1}{2}+\cdots+\frac{1}{r} \qquad \cdots(4)$$

又由于 $\quad 1=\lim\limits_{n\to\infty}(1+\frac{1}{n})^n$

从而对任何自然数 n 有 $\quad 1+\frac{1}{n}\leqslant e^{\frac{1}{n}}$

取对数得 $\ln(1+\frac{1}{n})\leqslant\frac{1}{n}$

分别取 $n=1,2,\cdots,r$ 代入,我们得到

$$1+\frac{1}{2}+\cdots+\frac{1}{r}\geqslant\ln\frac{2}{1}+\ln\frac{3}{2}+\cdots+\ln\frac{r+1}{r}$$
$$=\ln(r+1)>\mathrm{Ln}r\quad(\text{对 } r\geqslant2)\qquad\cdots(5)$$

由(3)(4)(5)式得,对 $r\geqslant2$,

$$\pi(x)<\frac{x}{\ln(1+r)}+2^r+r$$

特别地,对于任给的 $\varepsilon>0$,我们可以取 r 适当大,使 $\ln r>\frac{2}{\varepsilon}$

$$\frac{\pi(x)}{x}<\frac{\varepsilon}{2}+\frac{2^r+r}{x}<\frac{\varepsilon}{2}+\frac{2^{r+1}}{x}$$

固定 r 后,再取 x 足够大,可使

$$\frac{2^{r+1}}{x}<\frac{\varepsilon}{2}$$

于是 x 是够大时总有 $0\leqslant\frac{\pi(x)}{x}<\varepsilon$

这就说明了 $\lim\limits_{x\to\infty}\frac{\pi(x)}{x}=0$

证明:设 a 为 s 中具有 $k(0\leqslant k\leqslant r)$ 个性质的元素,其具有的性质不妨设为 $p_1,p_2,\cdots,p_k$,则 a 在 $A_{i1}\cap A_{i2}\cap\cdots\cap A_{il}$ 的充要条件是性质 $p_{i1},p_{i2},\cdots,p_{il}$ 全取自 $p_1,p_2,\cdots,p_k$,故:

a 在 $\sum|A_{i1}\cap A_{i2}\cap\cdots\cap A_{im}|$ 中出现了 C_k^m 次;在 $\sum|A_{i1}\cap A_{i2}\cap\cdots\cap A_{im+1}|$ 中出现了 C_k^{m+1} 次,…,在 $\sum|A_{i1}\cap A_{i2}\cap\cdots\cap A_{il}|$ 中出现了 C_k^l 次,…。

所以 a 在公式右端被计入的总次数为:

$C_k^m-C_{m+1}^m\cdot C_k^{m+1}+\cdots+(-1)^{l-m}C_l^m\cdot C_k^l+\cdots+(-1)^{r-m}C_r^m\cdot C_k^r$

$=C_m^mC_k^m-C_{m+1}^m\cdot C_k^{m+1}+\cdots+(-1)^{l-m}C_l^m\cdot C_k^l+\cdots+(-$

$1)^{r-m}C_r^m C_k^r$ （ * ）

$\because$ 当 $k<m$ 时，$C_k^m=C_k^{m+1}=\cdots=C_k^{m+r}=0$

当 $l>k$ 时，$C_k^l=0$

$\therefore$ 当 $k<m$ 时，$*=0$

$k\geqslant m$ 时，$*=\sum_{l=m}^{k}(-1)^{l-m}C_k^l\cdot C_l^m=\begin{cases}1 & m=k\\ 0 & m<k\end{cases}$

从而可知 $*=\begin{cases}1 & m=k\\ 0 & m\neq k\end{cases}$

即 a 在公式右端被计入一次当且仅当 a 恰具有 m 个性质，定理得证。

练 习 三

1. 设 a、b 是两个给定的非零整数，且有整数 x、y，使得 $ax+by=1$。证明：若 $a|n$ 且 $b|n$ 则 $ab|n$

2. 设奇数 $n>1$，证明：n 是素数的充要条件是 n 不能表为三个或三个以上的相邻正整数之和。

3. 将 1,2,…,1986 随意排成一行，得到一个数，证明它不会是素数。

4. 一个五位数是某一个整数的 4 次方，且奇数位数字之和等于偶数位数字之和，求这个数。

5. 设 Ps 表示全部由 1 构成的 s 位（十进制）整数。试证若 Ps 是素数，则 s 也是素数。

6. 设 $n>2$，试让 n 与 $n!$ 之间至少有一个素数，并由此证明素数是无限集。

7. 某甲参加一种会议，会上有六位朋友，某甲和其中每一人在会上各相遇 12 次，和每两人各相遇 6 次，每三人各相遇 4 次，每四人各相遇 3 次，每五人各相遇 2 次，每六人各相遇 1 次，一人也没遇见的有 5 次，问某甲共参加几次会议？

8. 设有 n 个人，各标上从 1 到 n 这 n 个号码，另有 n 把椅子，也标上从 1 到 n 这 n 个号码，问，这 n 个人坐在这 n 把椅子上且满足第 $i(i=1,2\cdots n)$ 个人不坐第 i 把椅子时不同坐法有多少种？

9. 试求 $\{1,2,\cdots n\}$ 这几个数字的具有以下性质的无重复排列 $a_1,a_2\cdots a_n$ 的个数：对任一个 i。

$1\leqslant i\leqslant n-1$，有 $a_{i+1}\neq a_i+1$

10. 确定方程 $x_1+x_2+x_3=14$，$x_i\leqslant 8(i=1,2,3)$ 的非负整数解的个数。

11. 甲、乙、丙、丁四人去做 A,B,C,D 四项工作，但甲不会做 A，乙不会做 A 和 B，丙不会做 B 和 C，丁不会做 C，若要求每人必

须做一项工作,问有多少种不同的安排方法?

12. 设 $n>2$,求证:如果 k^2+k+n 对于整数 k,($0\leqslant k\leqslant\sqrt{n/3}$)是素数,则 k^2+k+n 对于满足 $0\leqslant k\leqslant n-2$ 的整数 k 都是素数。

13. 设 p 个素数 $a_1,a_2,\cdots a_p$,构成递增的等差数列,且 $a_1>p$,证明如果 p 为素数,则 $p|d$,d 是公差。

第二章　算术基本定理

§1　带余除法

1.1　带余除法

初等数论的证明中最重要、最基本、最直接的工具就是下面的带余除法。

定理 2.1　设 a,b 是两个整数,其中 $b>0$,则存在两个唯一的整数 q 及 r,使得 $a=bq+r,0\leqslant r<b$　　　(1)成立。

证明:作整数序列……, $-3b,-2b,-b,0,b,2b,3b,\cdots$,则 a 必在上述序列的某两项之间,即 $\exists q\in Z$,使得 $qb\leqslant a<(q+1)b$ 成立。令 $a-qb=r$ 即可得 $a=bq+r,0\leqslant r<b$。

设 q_1,r_1 是满足(1)的另一对整数,因为 $a=bq_1+r_1=bq+r$,于是有 $b(q-q_1)=r_1-r$,故 $b|q-q_1|=|r_1-r|$。由于 r 及 r_1 是小于 b 的非负整数,所以上式右端是小于 b 的,如果 $q\neq q_1$,则上式左边大于等于 b,矛盾。因此 $q=q_1,r=r_1$。

定义 2.1　(1)中的 q 叫做 a 被 b 除得的不完全商,r 叫做 a 被 b 除的余数,也叫做非负最小剩余,常记作$\langle a\rangle_b=r$,在不致引起混淆的情况下,$\langle a\rangle_b$ 中的 b 常略去不写。我们有下面的定理

定理 2.2　对于整数 a_1,a_2,b,其中 $b>0$,有

$$(1)\ \langle a_1+a_2\rangle=\langle\langle a_1\rangle+\langle a_2\rangle\rangle$$

$$(2)\ \langle a_1-a_2\rangle=\langle\langle a_1\rangle-\langle a_2\rangle\rangle$$

$$(3)\ \langle a_1a_2\rangle=\langle\langle a_1\rangle\langle a_2\rangle\rangle$$

证明:　(1) 设 $a_1=bq_1+\langle a_1\rangle,a_2=bq_2+\langle a_2\rangle,\langle a_1\rangle+\langle a_2\rangle=bq_3+\langle\langle a_1\rangle+\langle a_2\rangle\rangle$

则

$$a_1+a_2=b(q_1+q_2)+\langle a_1\rangle+\langle a_2\rangle$$
$$=b(q_1+q_2+q_3)+\langle\langle a_1\rangle+\langle a_2\rangle\rangle$$

由定理 2.1 即可证得(1)。

类似地可以证明(2),(3)。

例 1 一个自然数 a 除 63,91,291 所得的余数之和为 10,求 a。

解:设 $63=aq_1+r_1, 91=aq_2+r_2, 291=aq_3+r_3, r_1+r_2+r_3=10$

由 $445=a(q_1+q_2+q_3)+10$,则 $a(q_1+q_2+q_3)=435=5\times3\times29$,由抽屉原则必有某个 $r_1>3$,故 $3<a<63$。由上式知 $a\in\{5,15,29\}$,经检验可知 $a=15$ 或 $a=29$。

例 2 已知等差数列的各项均是整数,它的公差是不能被 5 整除的奇数。求证这个数列的任何连续十项中必有一项能被 10 整除。

证明:设此等差数列的公差为 d,不妨设 $a_1,a_2,a_3\cdots a_{10}$为任意连续的十项,并设 $a_1=10q_1+r_i$,其中 q_i,r_i 都是整数。$0\leqslant r_i<10, i=1,2,\cdots,10$。当 $0\leqslant j<k\leqslant9$ 时,因为 $a_k-a_j=10(q_k-q_j)+r_k-r_j$,又因为 $a_k-a_j=(k-j)d$,所以有 $10(q_k-q_j)+r_k-r_j=(k-j)d$,即 $r_k-r_j=(k-j)d-10(q_k-q_j)$。又因为 $0\leqslant j<k\leqslant9$,所以 $k-j$ 不是 10 的倍数。又由已知 $2\nmid d, 5\nmid d$,从而 $10\nmid(k-j)$,显然 $10\mid10(q_k-q_j)$,故 $10\nmid r_k-r_j$,又 $10\leqslant r_i<10$,则 $-10\leqslant r_k-r_j\leqslant10$,从而 $r_k\neq r_j$,则 $r_1,r_2,r_3,\cdots r_{10}$是两两不等的十个数,但又 $r_i\in\{0,1,2\cdots,9\},(1\leqslant i\leqslant10)$,因此必有一个 $r_i=0$,故必有一个 a_i 是 10 的倍数。

例 3 已知 n 是一个使 $S_2(n)=\sum_{i=1}^{n}i^2$ 不能被 5 整除的自然数。试求 $S_1(n)=\sum_{i=1}^{n}i$ 被 5 除的余数。

解:若 $n=5k+r$,则 $S_1(n)$ 与 $S_1(r)$ 被 5 除的余数相同,$S_2(n)$与 $S_2(r)$被 5 除的余数相同。故只要求出 $S_2(r)$被 5 除的余

数即可。

而(0,1,2,3,4),(5,6,7,8,9),(10,11,12,13,14)……我们仅研究前五个数即可。由 $n^2=(5k+r)^2=25k^2+10kr+r^2$,则 $5\mid n^2-r^2$,即 $5\mid S_2(n)-S_2(r)$。又 $\sum_{i=1}^{4}i^2=30$, $S_2(0)=0$, $S_2(1)=1$, $S_2(2)=5\times1+0$, $S_2(3)=14=5\times2+4$, $S_2(4)=30=5\times6+0$,所以 $S_2(r)$被 5 除的余数是 0,1 或 4。又 $5\nmid S_2(n)$,即 $5\nmid S_2(r)$,所以有 $S_2(r)=5\times q+1$ 或 $S_2(r)=5\times q+4$,从而 $r=1$ 或 $r=3$,即 $S_1(n)$被 5 除的余数是 1。

例 4 $\overline{a_1a_2\cdots a_{1999}a_{2000}}$是按如下规则写出的一个两千位的自然数:先写 a_1 再写 $a_2,a_3\cdots$,当 a_i 已写出,再写 a_{i+1}时要求$\overline{a_ia_{i+1}}$是 17 或 23 的倍数 $i=1,2,\cdots1999$ 如果写出的数中有 1,9,8,7 这四个数码,求证:这个两千位数必是合数。

证明:两位数中 17 的倍数有:17,34,51,68,85。两位数中 23 的倍数有 23,46,69,92。顺序写下去,容易发现:当一个数码确定后,按规则出现 6→9→2→3→4→6→9 循环。但若出现 6→8→5→1→7,则循环中止。显然 $a_1\neq0$, $a_{2000}=7$ 倒推回去 $a_{1999}=1$, $a_{1998}=5$, $a_{1997}=8$, $a_{1996}=6$, $a_{1995}=4$, $a_{1994}=3$, $a_{1993}=2$, $a_{1992}=9$, $a_{1991}=6$……,每五个一循环。$2000=5\times400=5\times399+5$,即 $399(6+9+2+3+4)+6+8+5+1+7=\sum_{i=1}^{2000}a_i$, $\sum_{i=1}^{2000}a_i=3(8\times399+9)$,则 $3\mid\sum_{i=1}^{2000}a_i$,所以这个两千位数有因子 3,是合数。

1.2 整数的分类

由定理 2.1,我们知道:任何一个整数被 a(a>0)除后所得的非负最小剩余数是且仅是 0,1,2,…a-1 这 a 个数中的一个。由此我们就可以将整数进行分类。

设 $a\geqslant2$ 是给定的正整数,$j=0,1,2\cdots a-1$,对给定的 j,被 a 除后余数等于 j 的全体整数是 $S_{a,j}=\{ka+j\}$, $k=0,\pm1,\pm2\cdots$。显然有下列性质:

(1) 当 $0\leqslant j\neq j'\leqslant a-1$ 时，$S_{a,j}\cap S_{a,j'}=\phi$；

(2) $S_{a,0}\cup S_{a,1}\cup\cdots\cup S_{a,a-1}=Z$。

即全体整数按被 a 除后所得的非负最小剩余数来分类，分成了两两不相交的 a 个类。

当 a=2 时，就是熟知的奇、偶两大类。即 $S_{2,0}=\{2k,k\in Z\}$ $=\{$偶数$\}$，$S_{2,1}=\{2k+1,k\in Z\}=\{$奇数$\}$。

当 a=3 时，任何整数被 3 除得的余数是 0,1,2 之一，即每个整数都是 3k,3k+1,3k+2 之一的形式，其中 $k\in Z$。即 $S_{3,0}=\{3k,k\in Z\}$，$S_{3,1}=\{3k+1,k\in Z\}$，$S_{3,2}=\{3k+2,k\in Z\}$。

例 1 证明(1) $S_{2,0}\cap S_{3,0}=S_{6,0}$；

(2) $S_{2,1}=S_{6,1}\cup S_{6,3}\cup S_{6,5}$

证明：(1) "$\Leftarrow$"显然。

"$\Rightarrow$"设 a=2k 且 a=3h，$k,h\in Z$ 由 2k=3h 知 h=2(k−h)

所以 a=6(k−h)，则 6|a，$a\in S_{6,0}$。因此 $S_{2,0}\cap S_{3,0}=S_{6,0}$。

(2) 设 $n\in S_{2,1}$即 n=2k+1，$k\in Z$，则 k 必为下列三者之一：3h,3h+1,3h+2，$h\in Z$。因而必有 n=6h+1,6h+3 或 6h+5。反之显然成立。因此 $S_{2,1}=S_{6,1}\cup S_{6,3}\cup S_{6,5}$。

例 2 设 a>2 是奇数，证明：(1) 一定存在正整数 $d\leqslant a-1$ 使 $a|2^d-1$。(2) 设 d_0 是满足(1)的最小的 d，那么，$a|2^h-1$，($h\in N$)的充要条件是 $d_0|h$。

证明：(1) 考虑以下的 a 个数：$2^0,2^1,\cdots2^{a-1}$，由已知 $a\nmid 2^j$，($0\leqslant j<a$)，故设 $2^j=q_ja+r_j$，$0<r_j<a$。所以 a 个余数 $r_0,r_1,r_2\cdots r_{a-1}\in\{1,2\cdots,a-1\}$。由抽屉原则存在 i,k 使得 $r_i=r_k$，$0\leqslant i<k\leqslant a-1$，则有 $a(q_k-q_i)=2^i(2^{k-i}-1)$，令 $d=k-i\leqslant a-1$，则 $a|2^d-1$。

(2) 充分性显然。下证必要性。设 $j=qd_0+r$，$0\leqslant r<d_0$，则 $2^h-1=2^{qd+r}-1-2^r+2^r=2^r(2^{qd_0}-1)+(2^r-1)$。由 $a|2^h-1$

及 a|$2^{qd_0}-1$ 可得 a|2^r-1,由 d_0 的最小性知 r=0,即 d_0|h。

例 3 已知一个正整数,将其数字相加,其和可为一位数或多位数。如不是一位数,再将其和的数字相加,按此做下去,最后得到一位数为止,若该一位数是 2,3,5,6,8 中的一个,证明原给的整数不可能是完全平方数。

说明:任一整数都可表示成下列形式之一:9k,9k+1,…9k+8($k\in Z$)。这九种形式的数平方后被 9 除的余数为 0,1,4 或 7。反设所给的数为 $n^2(n\in N)$,记 n^2 的数字和为 a_1,易证 $9|(n^2-a_1)$,设 a_1 的数字和为 a_2,则 $9|(a_1-a_2)$,所以 $9|(n^2-a_2)$,……,继续下去,最后所得的一位数与 n^2 被 9 除的余数相等,所以这个一位数只能是 0,1,4,7 之一,与题设矛盾。

1.3 P 进制

我们常用的是十进制数,即一个十进制的自然数 $\overline{a_na_{n-1}\cdots a_1a_0}$ 可以表示为 $a_n10^n+a_{n-1}10^{n-1}+\cdots+a_110+a_0$,其中 $a_i\in\{0,1,2\cdots,9\}$,$0\leqslant i\leqslant n$,并且 $a_n\neq 0$。

例如,由于 $1998=1\times10^3+9\times10^2+9\times10+8$,而这种表示法可以用相同的除数 10 连续除而得:

$$
\begin{array}{r|l l}
10 & 1998 & \\
10 & 199 & \cdots 8 \\
10 & 19 & \cdots 9 \\
10 & 1 & \cdots 9 \\
 & 0 &
\end{array}
$$

其实,如果用相同的除数 P(P≥2)连续除某个数,就可得到这个数的 P 进制表示。关于 P 进制有下面的定理:

定理 2.3 设 P≥2 是整数,则任意正整数 a 唯一地被表示为 $a=a_np^n+a_{n-1}p^{n-1}+\cdots+a_1p+a_0$,$a_i\in N$,$0<a_n<p$,$0\leqslant a_i<p$,$i=0,1,2,\cdots n-1$(1)。

证明:存在性

因为 a,p 均为正整数,故有非负整数 q_1,a_0 使 $a=q_1p+a_0$,$0\leqslant a_0<p$。

若 $q_1=0$ 则 $a=a_0<p$ 已表示为(1)的形式。若 $0\neq q_1<p$，则令 $q_1=a_1$，故 $a=a_1p+a_0$，也表示为(1)的形式。若 $q_1>p$，则存在 $q_2,a_1\in Z$ 使 $q_1=q_2p+a_1$，$0\leq a_1<p$，$q_2\neq 0$，由此 $a=q_2p^2+a_1p+a_0$。若 $0<q_2<p$，令 $q_2=a_2$ 则 $a=a_2p^2+a_1p+a_0$，表示为(1)的形式。若 $q_2>p$，则存在 $q_3,b_2\in Z$ 使 $q_2=q_3p+a_2$，$0\leq a_2<p$，$q_3\neq 0$，则 $a=q_3p^3+a_2p^2+a_1p+a_0$。依此下去，因为 $q_1>q_2>q_3>\cdots$，故最后必有正整数 $q_n<pq_n=a_n$，使 $a=a_np^n+a_{n-1}p^{n-1}+\cdots+a_1p+a_0$，其中 $0<a_n<p$，$0\leq a_i<p$，$i=0,1,2,\cdots n-1$。

唯一性：

若 a 即可以表示成：

$a=a_np^n+a_{n-1}p^{n-1}+\cdots+a_1p+a_0$，$a_i\in N$，$0<a_n<p$，$0\leq a_i<p$，$i=0,1,2,\cdots n-1$

又可以表示成：

$a=b_np^n+b_{n-1}p^{n-1}+\cdots+b_1p+b_0$，$b_i\in N$，$0<b_n<p$，$0\leq b_i<$，$i=0,1,2,\cdots n-1$

则 $P|(a_0-b_0)$，又 $0<a_0<p$，$0<b_0<p$ $\therefore a_0-b_0$ 即 $a_0=b_0$。同理可证 $a_i=b_i(i=1,2,\cdots n)$

即 a 可唯一表示成 $a_np^n+a_{n-1}p^{n-1}+\cdots+a_1p+a_0$，$a_i\in N$，$0<a_n<p$，$0\leq a_i<0$，$i=0,1,2,\cdots n-1$

例 1 设 N 为正整数集，在 N 上定义函数如下：

(1) $f(1)=1$，$f(3)=3$；

(2) 对 $n\in N$，有 $f(2n)=f(n)$，$f(4n+1)=2f(2n+1)-f(n)$，$f(4n+3)=3f(2n+1)-2f(n)$。

试问有多少个 n，使 $n\leqslant 1988$ 且 $f(n)=n$。

解：由条件(1)和(2)可得：

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$f(n)$	1	1	3	1	5	3	7	1	9	5	13	3	11	7	15	1	17

观察发现，在 $n \leqslant 17$ 的范围内，有

$$f(2^k)=1, f(2^k-1)=2^k-1, f(2^k+1)=2^k+1。$$

显然，满足 $f(n)=n$ 的数不仅是 $2^k \pm 1$ 型，如 $f(21)=21$。这启发我们从二进制的角度来讨论问题，将上面表格中的数改为二进制表示，便有：

n	1	10	11	100	101	110	111	1000	1001	1011	1100	1101	1111	10000
$f(n)$	1	01	11	001	101	011	111	0001	1001	1101	0011	1011	1111	00001

从表中可以看出当 $n=(a_l,a_{l-1},\cdots,a_1,a_0)_2$ 时，似乎有 $f(n)=(a_0,a_1,\cdots,a_{l-1},a_l)_2$，$a_l=1$。$f(n)$ 即是把 n 的二进制倒过来写。

因为 $f(2n)=f(n)$，所以只须考虑 n 为奇数的情形。由已知(1)可见，$n=1$ 或 3 时结论成立。设命题对 $n<l$ 时成立，下证 $n=l$ 时命题也成立。

(1) 设 $l=4k+1$，$l=\overline{(t_1,t_2,\cdots,t_m01)_2}$，$t_i\in\{0,1\}$，$i=1,2,\cdots m$，于是 $k=\overline{(t_1,t_2,\cdots,t_m)_2}$，$2k+1=\overline{(t_1,t_2,\cdots,t_m1)_2}$。

所以，由(2)及归纳假设有

$$\begin{aligned} f(4k+1) &= 2f(2k+1)-f(k) \\ &= 2\overline{(1t_m,t_{m-1},\cdots,t_1)_2}-\overline{(t_m,t_{m-1},\cdots,t_1)_2} \\ &= \overline{(10t_m,t_{m-1},\cdots,t_1)_2} \end{aligned}$$

(2) 设 $l=4k+3$，则 $l=\overline{(t_1,t_2,\cdots,t_m11)_2}$，由(2)及归纳假设有

$$\begin{aligned} f(4k+3) &= 3f(2k+1)-2f(k) \\ &= 2f(2k+1)+f(2k+1)-2f(k) \\ &= 2\overline{(1t_m,t_{m-1},\cdots,t_10)_2}+\overline{(1t_m,t_{m-1},\cdots,t_1)_2} \\ &\quad -\overline{(t_m,t_{m-1},\cdots,t_10)_2} \\ &= \overline{(11t_m,t_{m-1},\cdots,t_1)_2} \end{aligned}$$

这说明了，当 $n=l$ 时命题成立。也就是说明了对于 $n=$

$\overline{(t_1,t_2,\cdots,t_m)_2}$, $f(n)=n \Leftrightarrow \overline{(t_1,t_2,\cdots,t_m)_2}=\overline{(t_m,t_{m-1},\cdots,t_1)_2}$。我们称具有这种性质的数为二进对称的。易证无论 $m=2m_1$,还是 $m=2m_1-1$,恰有 m 位的二进对称数的个数都恰为 2^{m_1-1}。因为 $1988=(11111000100)_2$,所以不大于 2^{11} 的对称数有

$$2(1+1+4+8+16)+2^5=94\text{ 个。}$$

又 $2^{11}=2048$,对当 $1988<n<2048$,对称数只有两个,即 $(11111011111)_2$,$(11111111111)_2$。所以,满足 $n\leqslant 1988$ 且 $f(n)=n$ 的数 n 共有 92 个。

§2 最大公约数和最小公倍数

2.1 最大公约数和最小公倍数

定义 2.2 设 $n\geqslant 2$ 是整数,若 $a_1,a_2,\cdots,a_n$ 不全为零,且 $d\mid a_1,d\mid a_2,\cdots,d\mid a_n$ 则 d 叫做 $a_1,a_2,\cdots,a_n$ 的公约数,其中最大者叫做最大公约数,用记号 $(a_1,a_2,\cdots,a_n)$ 表示。

定义 2.3 若 $(a_1,a_2,\cdots,a_n)=1$,就说 $a_1,a_2,\cdots,a_n$ 互素。

$a_1,a_2,\cdots,a_n$ 互素与两两互素是不同的概念。例如,6,10,25 互素,但 $(6,10)=2$,$(10,25)=5$,即 6 与 10,10 与 25 均不互素。

定义 2.4 设 $n\geqslant 2$ 是整数,若 $a_1\mid m,a_2\mid m,\cdots,a_n\mid m$ 则 m 叫做 $a_1,a_2,\cdots,a_n$ 的公倍数。正公倍数中最小者叫做最小公倍数,用记号 $[a_1,a_2,\cdots,a_n]$ 表示。

由定义 2.4 可以推出如下性质:

定理 2.4 (1) $(a_1,a_2)=(a_2,a_1)=(-a_1,a_2)$;

一般地,$(a_1,a_2,\cdots,a_i,\cdots,a_k)=(a_i,a_2,\cdots,a_1,\cdots,a_k)=(-a_1,a_2,\cdots,a_k)$;

(2) 若 $a_1\mid a_j,j=2,\cdots,k$,则 $(a_1,a_2)=(a_1,a_2,\cdots,a_k)=|a_1|$;

(3) 对任意整数 x,$(a_1,a_2)=(a_1,a_2,a_1x)$;

$(a_1, a_2, \cdots, a_k) = (a_1, a_2, \cdots, a_k, a_1 x)$;

(4) 对任意整数 x, $(a_1, a_2) = (a_1, a_2 + a_1 x)$,

$(a_1, a_2, a_3, \cdots, a_k) = (a_1, a_2 + a_1 x, a_3, \cdots, a_k)$;

定理 2.5 $[a_1, a_2] = [a_2, a_1] = [-a_1, a_2]$;一般地有,

$[a_1, a_2, \cdots, a_i, \cdots, a_k] = [a_i, a_2, \cdots, a_1, \cdots, a_k] = [-a_1, a_2, \cdots, a_k]$;

(2) 若 $a_2 | a_1$,则 $[a_1, a_2] = |a_1|$;若 $a_j | a_1$, $j = 2, \cdots, k$ 则 $[a_1, a_2, \cdots, a_k] = |a_1|$;

(3) 对任意的 $d | a_1$, $[a_1, a_2] = [a_1, a_2, d]$; $[a_1, a_2, \cdots, a_k] = [a_1, a_2, \cdots, a_k, d]$。

证明留给读者。

定理 2.6 一组数的公倍数恒是其最小公倍数的倍数。

证明:设 $a_1, a_2, \cdots, a_n$ 的最小公倍数为 m,即 $[a_1, a_2, \cdots, a_n] = m$,并设 m_1 为 $a_1, a_2, \cdots, a_n$ 的任一公倍数。由定理 2.4 有 $m_1 = mq + r$, $0 \leqslant r < m$,又 $a_1, a_2, \cdots, a_n$ 均能整除 m_1 与 m,有 $a_1, a_2, \cdots, a_n$ 均能整除 r,即 r 也是 $a_1, a_2, \cdots, a_n$ 的公倍数,若 $r > 0$,则与 m 的最小性矛盾。所以 $r = 0$,即 $m_1 = mq$。

定理 2.7 一组数的最大公约数是它们的全体公约数的最小公倍数。或者说,一组数的最大公约数的全体约数就是这组数的全体公约数。

证明:设 $d_1, d_2, d_3, \cdots, d_m$ 是 $a_1, a_2, \cdots, a_n$ 的全体公约数,并设其最小公倍数为 $d = [d_1, d_2, d_3, \cdots d_m]$。$d$ 是 $d_1, d_2, d_3, \cdots d_m$ 的最大公约数,而 a_i 为 $d_1, d_2, d_3, \cdots d_m$ 的公倍数,由前面定理知 $d | a_1, d | a_2, \cdots, d | a_n$。所以,$d$ 为 $a_1, a_2, \cdots, a_n$ 的公约数。因此,d 为 $d_1, d_2, d_3, \cdots d_n$ 中的某一个。又 d 是 $d_1, d_2, d_3, \cdots d_m$ 的最小公倍数,所以 d 是 $d_1, d_2, d_3, \cdots d_m$ 中最大者。于是,最大公约数是全体公约数的最小公倍数。

定理 2.8 设 a, b, c 是任意三个不全为 0 的整数,且 $a = bq$

$+c, q\in Z$,则$(a,b)=(b,c)$。

证明: 因为,$(a,b)|a,(a,b)|b$

所以,$(a,b)|c$

所以,$(a,b)\leqslant(b,c)$

同理可证$(b,c)\leqslant(a,b)$

所以,$(a,b)=(b,c)$。

关于求多个数的最大公约数和最小公倍数,有如下性质:

性质:(1) $(a_1,a_2,\cdots,a_n)=((a_1,a_2,\cdots,a_s),(a_{s+1},\cdots a_n))$, $1\leqslant s<n$

(2) $[a_1,a_2,\cdots,a_n]=[[a_1,a_2,\cdots,a_s],[a_{s+1},\cdots a_n]]$, $1\leqslant s<n$

(3) $[ma_1,ma_2,\cdots,ma_n]=m[a_1,a_2,\cdots,a_n]$

这三个性质的证明留给读者。

例 1 对于任意自然数 n,证明分数$\frac{21n+4}{14n+3}$不可约。

证明: $\because(21n+4,14n+3)=(7n+1,14n+3)=(7n+1,7n+2)=1$

$\therefore\frac{21n+4}{14n+3}$不可约。

例 2 设 $m>0,n>0$,且 m 是奇数,证明$(2^m-1,2^n+1)=1$。

证明: 设$(2^m-1,2^n+1)=d$,则存在 $s,t,\in Z$ 使 $2^m=sd+1,2^n=td+1$。

由此 $2^{mn}=(sd+1)^n,2^{mn}=(td+1)^m$,

则 $2^{mn}=pd+1=qd-1,p,q\in Z$,

所以,$(q-p)d=2$,

所以,$d|2$,因此 $d=1$ 或 2

又因为 $2^m-1,2^n+1$ 都是奇数,所以 $d=1$

即$(2^m-1,2^n+1)=1$。

例 3 设 $u_n=497+n^2$,函数 $f(x)$定义在自然数集上,且对任意一自然数 n,$f(n)$为 u_n 与 u_{n+1}的最大公约数,求函数 $f(x)$

的值域。

解：一般的有，$u_n=p+n^2$，$(n\in N)$。

首先证明 $f(n)|2n+1$，$f(n)|4p+1$。

因为，$f(n)|p+n^2$，$f(n)|p+(n+1)^2$，

又 $2n+1=p+(n+1)^2-(p+n^2)$，

所以，$f(n)|2n+1$，又 $f(n)|2(p+n^2)$，

所以，$f(n)|2p-n$。

又 $4p+1=2n+1+2(2p-n)$，

所以，$f(n)|4p+1$。

其次证明，对 $4p+1$ 的任意一个正因数 $2r+1$，有 $f(r)=2r+1$。

由 $f(r)|2r+1$，只要证明 $2r+1|f(r)$。

因为，$4(r^2+p)=(2r+1)(2r-1)+(4p+1)$，

所以，$2r+1|4(r^2+p)$。

又因为，$(2r+1,4)=1$，

所以，$2r+1|(r^2+p)$。　　　　(1)

因为，$p+(r^2+1)=(r^2+p)+2r+1$，

所以，$2r+1|p+(r_2+1)$。　　　　(2)

由(1)，(2)知 $2r+1|f(r)$。

综上所述，对于 $u_n=p+n^2$，$f(x)$的值域为 $4p+1$ 的正因数的集合。

当 $p=497$ 时，$4p+1=3^2\times13\times17$，$f(x)$的值域为$\{1,3,9,13,17,39,51,117,153,221,663,1989\}$。

2.2　辗转相除法

由定理 2.6，我们可以归纳出求最大公约数的方法——辗转相除法。辗转相除法也叫做 Euclid 算法。

定理 2.9　设 u_0,u_1 是给定的两个整数，$u_1\neq0$，$u_1\neq u_0$，可以得到下面的 $k+1$ 个等式

$u_0=q_0u_1+u_2, 0<u_2<|u_1|$

$$
\begin{aligned}
&u_1 = q_1 u_2 + u_3, 0 < u_3 < u_2 \\
&u_2 = q_2 u_3 + u_4, 0 < u_4 < u_3 \\
&\cdots\cdots \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (1) \\
&u_{k-2} = q_{k-2} u_{k-1} + u_k, 0 < u_k < u_{k-1} \\
&u_{k-1} = q_{k-1} u_k + u_{k+1}, 0 < u_{k+1} < u_k \\
&u_k = q_k u_{k+1}
\end{aligned}
$$

证明:因为 $u_1 \nmid u_0$,故存在 q_0, u_2,使 $u_0 = q_0 u_1 + u_2, 0 < u_2 < |u_1|$ 成立。如果 $u_2 | u_1$,则定理对 $k=1$ 成立。如果 $u_2 \nmid u_1$ 就得到(1)中第二个式子。依次下去,有 $|u_1| > u_2 > u_3 > \cdots > u_{j+1} > 0$,及(1)的前 j 个等式成立。若 $u_{j+1} | u_j$,则定理对 $k=j$ 成立;若 $u_{j+1} \nmid u_j$,则继续对 u_{j+1}, u_j 应用定理 2.8,由于 u_1 的正整数只有有限个,故这个过程不会无限做下去,一定会出现某个 k,要么 $u_{k+1} | u_k$,要么 $(u_{k+1}, u_k) = 1$。

定理 2.10　在定理 2.9 的符号和条件下,有:

(1) $u_{k+1} = (u_0, u_1)$;

(2) $d | u_0$ 且 $d | u_1$ 的充要条件是 $d | u_{k+1}$;

(3) 存在整数 x_0, x_1,使得下式成立

$u_{k+1} = x_0 u_0 + x_1 u_1$

证明:由定理 2.9 中(1)式的最后一式开始,依次向前推,可得 $u_{k+1} = (u_{k+1}, u_k) = (u_k, u_{k-1}) = (u_{k-1}, u_{k-2}) = \cdots = (u_2, u_1) = (u_1, u_0)$

由此证明了(1)。由(1)即可得(2)。

由定理 2.9 的第 k 式知,$u_{k+1} = u_{k-1} - q_{k-1} u_k$,及 $u_k = u_{k-2} - q_{k-2} u_{k-1}$,则 $u_{k+1} = u_{k-1} - q_{k-1}(u_{k-2} - q_{k-2} u_{k-1})$,消去了 u_k,依次利用定理 2.9 的各式,可相应地消去 $u_{k-1}, u_{k-2}, \cdots u_3, u_2$,最后得到 u_{k+1}关于 u_0 和 u_1 表达式。即 u_{k+1}可以表为关于 u_0 和 u_1 的整系数线性组合。显然,当 $u_1 | u_0$ 时,定理 2.10 也成立。

推论:对于任意的两个整数 a 和 b,$(a,b)=1$ 的充要条件是存在 $s,t\in Z$,使 $as+bt=1$。

证明:"⇒"由定理 2.10 可得。

"⇐"设 $(a,b)=d$,因为,$as+bt=1$,

由 $d|a$,$d|b$ 可知 $d|as+bt$,

所以,$d|1$,又 $d>0$,

所以,$d=1$,即 $(a,b)=1$。

定理 2.11 设 b,c 中至少有一个不为零,且 $(a,c)=1$,则 $(ab,c)=(b,c)$。

证明:因为 $(a,c)=1$,则存在 $s,t\in Z$,使 $as+ct=1$。于是 $(ab)s+c(bt)=b$,记 $d_1=(ab,c)$,$d_2=(b,c)$,则 $d_1|b$。所以 d_1 是 b 和 c 的公因数,故 $d_1|d_2$。又 $d_2|b$,知 $d_2|ab$,所以 d_2 是 ab 和 c 的公因数。所以 $d_2|d_1$,$d_1=d_2$。

推论 1:若 $(a,b_1)=(a,b_2)=\cdots=(a,b_n)=1$,则 $(a,b_1b_2\cdots b_n)=1$。

推论 2:设 m,n 为正整数,若 $(a,b)=1$,则 $(a^m,b^n)=1$。

推论 3:设 $(a_i,b_j)=1$,$i=1,2,\cdots,m$,$j=1,2,\cdots n$,则 $(a_1a_2\cdots a_m,b_1b_2\cdots b_n)=1$。

定理 2.12 若 $(a,c)=1$,且 $c|ab$,则 $c|b$。

证明:由定理 2.6 及 $c|ab$ 知 $(b,c)=(ab,c)=|c|$。于是 $|c||b$,故 $c|b$。

推论 1:若 $(a,b)=1$,且 $a|b^2$,则 $a|b$。

推论 2:$n\geqslant 2$,若 $a|a_1a_2\cdots a_n$,且 $(a,a_1)=(a,a_2)=\cdots=(a,a_{n-1})=1$,则必有 $a|a_n$。

例 1 求(216,378)

解:$378=216\times 1+162$

$216=162\times 1+54$

$162=54\times 3$

所以,$(216,378)=(216,162)=(162,54)=54$。

将上述过程逆推回去,就可得到 54 关于 216 和 378 的表达式。

$$
\begin{aligned}
54 &= 216 - 162 \\
&= 216 - (378 - 216) \\
&= 2 \times 216 - 378
\end{aligned}
$$

定理 2.13　设 a, b 不同时为零,则 $(a,b) = (a, b - ax) = (a - bx, b)$ 对任意 x 都成立。

证明:设 d 是 a 和 b 的公约数,则 $d \mid b - ax, d \mid a - bx$。所以 d 是 a 和 $b - ax$ 的公约数,d 也是 b 和 $a - bx$ 的公约数。若 d 是 a 和 $b - ax$ 的公约数,则 $d \mid b$,所以 d 是 a 和 b 的公约数。同理,若 d 是 $a - bx$ 和 b 的公约数,则 $d \mid a$,即 d 是 a 和 b 的公约数。所以 a 和 b 的公约数集等同于 a 和 $b - ax$ 的公约数集,等同于 $a - bx$ 和 b 的公约数集。所以 $(a,b) = (a, b - ax) = (a - bx, b)$。

由此例 1 也可以写成:

$$
\begin{aligned}
(216,378) &= (378 - 216, 216) = (216, 162) = (216 - 162, 162) \\
&= (162, 54) = (162 - 3 \times 54, 54) = (0, 54) = 54
\end{aligned}
$$

所以,$(216,378) = 54$。

并且,$54 = 216 - 162, 216 - (378 - 216) = 2 \times 216 - 378$。

例 2　设 n 为正整数,$M_n = 2^n - 1$ 称为梅森数(*Mersenne*),求证,$(M_a, M_b) = 1$ 的充要条件是 $(a,b) = 1$。

证明:"⇒"设 $d = (a,b)$,及 $a = dp, b = dq, d \in Z$,

所以,$2^a - 1 = (2^d)^p - 1 = (2^d - 1)N_1, N_1 \in Z$,

$2^b - 1 = (2^d)^q - 1 = (2^d - 1)N_2, N_2 \in Z$,

所以,$2^d - 1$ 是 $2^a - 1$ 和 $2^b - 1$ 的公因数。

因此,$2^d - 1 \mid 1$,所以 $2^d - 1 = 1$,故 $d = 1$,即 $(a,b) = 1$。

"⇐"不妨设 $a \geqslant b$,由带余除法得 $a = q_1 b + r_1, 0 \leqslant r_1 < b$,

所以,$M_a = 2^a - 1 = 2^{q_1 b + r_1} - 2^{r_1} + 2^{r_1} - 1 = 2^{r_1}(2^{q_1 b} - 1) + 2^{r_1} - 1$,

所以,$2^b - 1 \mid 2^{q_1 b} - 1$,

所以，$(2^a-1,2^b-1)=(2^b-1,2^{r_1}-1)$，且$(a,b)=(b,r_1)$。

若 $r_1=0$，则$(2^a-1,2^b-1)=2^{(a,b)}-1=1$，结论成立。

若 $r_1>0$，则继续对$(2^b-1,2^{r_1}-1)$作同样的讨论，由辗转相除法可知

$(2^a-1,2^b-1)=2^{(a,b)}-1$，又$(a,b)=1$，

所以，$(2^a-1,2^b-1)=1$。

2.3 $ab=(a,b)[a,b]$

设 a,b 是两个正整数，关于 a,b 的最大公约数与最小公倍数有下面的定理。

定理 2.14　两正整数之积等于其最大公约数与最小公倍数之积：

$$ab=(a,b)[a,b]。$$

证明：令$(a,b)=d,[a,b]=m$。因为 ab 是 a 与 b 的公倍数，故$\frac{ab}{m}$是整数。令$\frac{ab}{m}=g$，由此得$\frac{a}{g}=\frac{m}{b},\frac{b}{g}=\frac{m}{a}$。

此二式之右端均为整数，所以 g 为 a 与 b 之公约数。设 h 是 a,b 的任一公约数。令 $m'=\frac{ab}{h}$，则由 $m'=a\cdot\frac{b}{h}=b\cdot\frac{a}{h}$ 知 m' 为 a 与 b 的公倍数。所以

$$\frac{m'}{m}=\frac{\frac{ab}{h}}{\frac{ab}{g}}=\frac{g}{h}$$

是整数。即 a 与 b 的任一公约数 h 都能整除 g，这就是说，g 是 a 与 b 的最大公约数。即

$$g=\frac{ab}{m}=d,$$

亦即

$$ab=(a,b)[a,b]。$$

推论：若$(a,b)=1$，则$[a,b]=ab$。

这个定理说明求两个数的乘积可以转化成求这两个数的最大

公约数和最小公倍数。

定理 2.15 d 为 $a_1a_2\cdots a_n$ 的最大公约数的充分必要条件是 $\frac{a_1}{d},\frac{a_2}{d},\cdots,\frac{a_n}{d}$ 互素，即

$$(a_1,a_2,\cdots a_n)=d\Leftrightarrow\left(\frac{a_1}{d},\frac{a_2}{d},\cdots\frac{a_n}{d}\right)=1$$

证明："⇒"反证法。

已知 $(a_1,a_2,\cdots,a_n)=d$。若 $\left(\frac{a_1}{d},\frac{a_2}{d},\cdots,\frac{a_n}{d}\right)=a>1$，则 $\frac{a_1}{da},\frac{a_2}{da},\cdots,\frac{a_n}{da}$ 都是整数，即 $a_1,a_2,\cdots,a_n$ 的公约数 $da>d$，与假设矛盾，所以 $\left(\frac{a_1}{d},\frac{a_2}{d},\cdots,\frac{a_n}{d}\right)=1$。

"⇐"反证法。

已知 $\left(\frac{a_1}{d},\frac{a_2}{d},\cdots,\frac{a_n}{d}\right)=1$。若 $(a_1,a_2,\cdots a_n)\neq d$，则由已知，$d$ 为 $a_1,a_2,\cdots a_n$ 的公约数，所以 $(a_1,a_2,\cdots a_n)=dd_1>d$，这里 $d_1>1$。这就是说 $\frac{a_1}{d},\frac{a_2}{d},\cdots,\frac{a_n}{d}$ 有公约数 $d_1>1$，与假设 $\left(\frac{a_1}{d},\frac{a_2}{d},\cdots,\frac{a_n}{d}\right)=1$ 矛盾。所以 $(a_1,a_2,\cdots a_n)=d$。

定理 2.16 若 $(a_1,a_2,\cdots a_n)=d$，则

(1) $(ka_1,ka_2,\cdots ka_n)=kd$；

(2) $\left(\frac{a_1}{a},\frac{a_2}{a},\cdots,\frac{a_n}{a}\right)=\frac{d}{a}$，

其中 a 为 $a_1,a_2,\cdots,a_n$ 的公约数。

证明：(1) 应用定理 2.15，由 $(a_1,a_2,\cdots a_n)=d$，得 $\left(\frac{a_1}{d},\frac{a_2}{d},\cdots,\frac{a_n}{d}\right)=1$。即

$$\left(\frac{ka_1}{kd},\frac{ka_2}{kd},\cdots,\frac{ka_n}{kd}\right)=1$$

得

$$(ka_1, ka_2, \cdots ka_n) = kd。$$

（2）由$(a_1, a_2, \cdots a_n) = d$ 得

$$\left(\frac{a_1}{d}, \frac{a_2}{d}, \cdots, \frac{a_n}{d}\right) = 1$$

从而有

$$\left(\frac{\frac{a_1}{d}}{\frac{d}{a}}, \frac{\frac{a_2}{d}}{\frac{d}{a}}, \frac{\frac{a_n}{d}}{\frac{d}{a}}\right) = 1 \qquad 即，\left(\frac{a_1}{a}, \frac{a_2}{a}, \cdots, \frac{a_n}{a}\right) = \frac{d}{a}。$$

由此定理，可知，若 a 是$a_1, a_2, \cdots a_n$ 的公约数，则

$$(a_1, a_2, \cdots a_n) = \left(a \cdot \frac{a_1}{a}, a \cdot \frac{a_2}{a}, \cdots, a \cdot \frac{a_n}{a}\right)$$

$$= a\left(\frac{a_1}{a}, \frac{a_2}{a}, \cdots, \frac{a_n}{a}\right)。$$

这就是说，在求最大公约数时，可以把任何公约数提出来。

例 1 设 a, b 是自然数，在 $a, 2a, \cdots, ba$ 这 b 个数中，共有多少个 b 的倍数？

解：由于在 $a, 2a, \cdots, ba$ 中任意一个数都是 a 的倍数，故凡是 b 的倍数必是 a, b 的公倍数，也必是$[a, b]$的倍数，故 b 的倍数的个数为$\frac{ba}{[a, b]} = (a, b)$。

例 2 已知两数的平方和是 468，它们的最大公约数与最小公倍数的和是 42，求此两数。

解：设所求的两数为 x, y，且$(x, y) = d$，$[x, y] = \frac{xy}{d}$。由题意：

$$\begin{cases} x^2 + y^2 = 468 \\ d + \frac{xy}{d} = 42 \end{cases}$$

令 $x = dx_1 \quad y = dy_1 \quad (x_1, y_1) = 1$，

原方程组可化为：

$$\begin{cases} {x_1}^2+{y_1}^2=\dfrac{468}{d^2} & (1) \\ 1+x_1y_1=\dfrac{42}{d} & (2) \end{cases}$$

由$\dfrac{468}{d^2}$知 d 只能取 1,2,3,6,此时有

$$\begin{cases} {x_1}^2+{y_1}^2=117 \\ x_1y_1=20 \end{cases} \quad \begin{cases} {x_1}^2+{y_1}^2=52 \\ x_1y_1=13 \end{cases} \quad \begin{cases} {x_1}^2+{y_1}^2=13 \\ x_1y_1=6 \end{cases}$$

由此,仅当 $d=6, x_1=2, y_1=3$ 时方程组有解。所以,$x=12$, $y=18$。

例 3 设 $\phi\neq S\subset N$,且对加法封闭,自然数 m,d,对于 $x>m$,$x\in S$ 的充要条件是$d|x$。

证明:设 a_0 是 S 中最小的数,如果 a_0 整除 S 中所有的数,令 $d=a_0$。否则存在 $a_1\in S, a_0\neq a_1$,令 $d_1=(a_0,a_1)$,则 $d_1<a_0$。若 d_1 整除 S 中所有的数,令 $d=d_1$。否则在 S 中有 $a_2, d_1\neq a_2$。令 $d_2=(d_1,d_2)$,则 $d_2<d_1$。依此下去,由于 $a_0>d_1>d_2>\cdots$,所以经过有限步后这一过程必然停止。即存在 d_n 整除 S 中所有的数。令 $d=d_n$,即 $d=(a_1,a_2,\cdots,a_n)$,则存在 $u_0,u_1,\cdots,u_n\in Z$,使得下式成立:

$$u_0a_0+u_1a_1+\cdots+u_na_n=d \quad (1)。$$

(1) 式中的 u_i 可能是负的,若 $u_i<0$,则在(1)的两边加上 $\left(1+\dfrac{a_0}{d}\right)a_i(-u_i)$,因为 $d|a_i$,(1)式变为:$u'_0a_0+u'_1a_1+\cdots+u'_na_n=qd$,其中 $q\in N$, $u'_i\geqslant\max\left(0,-u_i\dfrac{a_0}{d}\right)$, $i=0,1,\cdots,n$。令 $m=qd$,则在 $n>m$,并且 $d|n$ 时,必有 $x\in S$。事实上,$x-m=q_0a_0+r$, $0\leqslant r<a_0$。

所以,$d|r$,

所以,$r=u''_0a_0+u''_1a_1+\cdots+u''_na_n=\dfrac{r}{d}d$,

其中，$u''_i=\frac{r}{d}u_i$，$0\leqslant i\leqslant n$，于是 $x=q_0a_0+m+r=q_0a_0+qd+r$。

所以，$x=q_0a_0+(u'_0+u''_0)a_0+(u'_1+u''_1)a_1+\cdots+(u'_n+u''_n)a_n$，由 S 对加法封闭，所以 $x\in S$。

§3 算术基本定理

3.1 算术基本定理

定理 2.17 设 p 是素数，$p|a_1a_2$，则 $p|a_1$ 或 $p|a_2$。

证明 Ⅰ：不妨设 $a_1>0,a_2>0$，若 $p\nmid a_1$，考虑数列 $a_1,2a_1,3a_1,\cdots,ka_1,\cdots$这数列中必有数可被 p 整除，如 pa_1。由最小数原理知，该数列中被 p 整除的数中必有一最小的，设为 na_1。显然有 $1<n\leqslant p$，下证 $n=p$。若不然，由带余除法知 $p=qn+r(1\leqslant r<n)$，$r\geqslant1$ 是因为 p 是素数，$n\nmid p$，故 $p|ra_1$，这和 na_1 的最小性矛盾。最后证 $p|a_2$，由带余除法知 $a_2=sp+t,0\leqslant t<p$，所以 $p|ta_1$，由 pa_1 的最小性，必有 $t=0$，则 $p|a_2$。

证明 Ⅱ：不妨设 $a_1\geqslant1,a_2\geqslant1$，用反证法，反设结论不成立，由最小数原理知，必存在最小的素数 p_0，使结论不成立，即存在 a_1,a_2，使得 $p_0|a_1a_2,p_0\nmid a_1,p_2\nmid a_2$。考虑所有这样的数对$\{a_1,a_2\}$组成的集合 T，由最小数原理知，必有 a_1^*,a_2^* 属于这集合，且使 $a_1^*a_2^*$ 最小。此时必有 $1<a_1^*<p_0,1<a_2^*<p_0$，否则，若 $a_1^*>p_0$，则由带余除法可得 $a_1^*=qp_0+r_1,0<r_1<p$，则数对$\{r_1,a_2^*\}$也属于集合 T。但 $r_1a_2^*<a_1^*a_2^*$，这和 $a_1^*a_2^*$ 的最小性矛盾。设 $a_1^*a_2^*=p_0c$，由前知 $2\leqslant c<p_0$，则有素数 $p_1|c$，由 $p_1<p_0$ 及 p_0 的最小性知，$p_1|a_1^*$ 和 $p_1|a_2^*$ 至少有一个成立，设 $p_1|a_1^*$，则有 $\left(\frac{a_1^*}{p_1}\right)a_2^*=p_0\left(\frac{c}{p_1}\right)$，显见数对$\{\frac{a_1^*}{p_1},a_2^*\}\in T$，与 $a_1^*a_2^*$ 的最小性矛盾。

由证明Ⅰ，Ⅱ不难得到一个简单的证明。

证明Ⅲ：若 $p\nmid a_1$，则$(p,a_1)=1$，又因为 $p|a_1a_2$，则必有 $p|a_2$。

推论 1　设 p 是素数，$p|a^2$，则 $p|a$。

推论 2　设 p 是素数，若 $p|a_1a_2\cdots a_r$，则在 $p|a_1,p|a_2,\cdots,p|a_r$ 中至少有一个成立。

定理 2.18 （算术基本定理） 设 $a>1$，则必有 $a=p_1p_2p_3\cdots p_s$　(1)，其中 $p_j(1\leqslant j\leqslant s)$是素数，且在不计次序的意义下，表达式(1)是唯一的。

证明Ⅰ：在第一章中我们证明了表达式(1)的存在性，下面来证明唯一性。

不妨设 $p_1\leqslant p_2\cdots\leqslant p_s$，若 a 还有表达式 $a=q_1q_2\cdots q_r,q_1\leqslant q_2\leqslant\cdots\leqslant q_r$，其中 $q_i(1\leqslant i\leqslant r)$是素数，下面证明 $r=s$，且 $p_j=q_j$ $(1\leqslant j\leqslant s)$，不妨设 $r\geqslant s$。由 $q_1|a=p_1p_2\cdots p_s$，则由定理 2.17 知必有个 p_j 满足 $q_1|p_j$，由于 q_1 和 p_j 是素数，故 $q_1=p_j$，同样地由 $p_1|a=q_1q_2\cdots q_r$ 知必有某个 q_i 满足 $p_1|q_i$，因此 $p_1=q_i$，由 $q_1\leqslant q_i=p_1\leqslant p_j$，故 $p_1=q_1$。则 $q_2q_3\cdots q_r=p_2p_3\cdots p_s$ 同理可得 $q_2=p_2,\cdots,q_s=p_s,q_{s+1}\cdots q_r=1$ 则必有 $r=s$，即不存在 $q_{s+1},\cdots,q_r$。

把式(1)中相同的素数合并，即得

$$a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}\quad p_1<p_2<\cdots<p_s \qquad (2)$$

(2) 式称为 a 的标准素因数分解式。简称标准分解式

证明Ⅱ：反证法。反设 $a_0>1$ 是使结论不成立的最小正整数，故 a_0 必有两种方法表示成素数之积，设为 $a_0=p_1p_2\cdots p_s=q_1q_2\cdots q_r$，其中 $p_j,q_i(1\leqslant j\leqslant s,1\leqslant i\leqslant r)$都是素数，不妨设 $p_1\leqslant p_2\leqslant\cdots\leqslant p_s,q_1\leqslant q_2\cdots\leqslant q_r$。显然，$a_0$ 不是素数，则必有：

$$s\geqslant 2,r\geqslant 2 \qquad (1)$$

其次由 a_0 的最小性可知，对任意的 j 和 i 必有

$$p_j\neq q_i \qquad (2)$$

不妨设 $q_1>p_1$，则有

$$1<b_0=a_0-p_1q_2\cdots q_r=(q_1-p_1)q_2\cdots q_r<a_0 \tag{3}$$

显然有 $p_1|b_0$,设 $b_0=p_1b_1$,设 b_0 的素数分解式为

$$b_0=p_1p_2'\cdots p_u',\ b_1=p'_2\cdots p'_u, \tag{4}$$

其中 $p'_2,\cdots,p'_u$ 是素数。当 $q_1-p_1=1$ 时,

$$b_0=q_2\cdots q_r \tag{5}$$

当 $q_1-p_1>1$ 时,必有 q_1-p_1 的素数分解式 $q_1-p_1=q_{11}\cdots q_{1\nu}$,$q_{1j}(1\leqslant j\leqslant\nu)$是素数。由此得到 b_0 的素数分解

$$b_0=q_{11}q_{12}\cdots q_{1\nu}q_2\cdots q_r \tag{6}$$

由 p_1,q_1 都是素数及 $q_1\neq p_1$ 知,$p_1\nmid q_1-p_1$,故在 b_0 的素数分解式(5)或(6)中不会出现 p_1,所以(5)或(6)是和(4)不同的素数分解式,但由(3)知,这和 a_0 的最小性矛盾。

定理 2.19　定理 2.17 和定理 2.18 等价。

证明:由定理 2.17 可推出定理 2.18。见定理 2.18 的证明Ⅰ。

下由定理 2.18 证定理 2.17。用反证法。

设有素数 p_0,正整数 a_1,a_2 满足 $p_0|a_1a_2,p_0\nmid a_1,p_0\nmid a_2$

显然有 $a_1\geqslant2,a_2\geqslant2,a_1a_2/p_0\geqslant2$,设

$$\begin{aligned}&a_1=p_{11}p_{12}\cdots p_{1r}\\&a_2=p_{21}p_{22}\cdots p_{2s}\\&a_1a_2/p_0=p_1p_2\cdots p_t,\end{aligned} \tag{1}$$

其中 $p_{1i},p_{2j},p_k(1\leqslant i\leqslant r,1\leqslant j\leqslant s,1\leqslant k\leqslant t)$是素数。由 $p_0\nmid a_1$ 知 $p_{1j}\neq p_0,(1\leqslant j\leqslant r)$,由 $p_0|a_2$ 知 $p_{2j}\neq p_0,(1\leqslant j\leqslant s)$。这样由(1)式就得到了 a_1a_2 的两种不同的素数分解式

$a_1a_2=p_{11}p_{12}\cdots p_{1r}p_{21}p_{22}\cdots p_{2s}$,

和 $a_1a_2=p_0p_1p_2\cdots p_t$,

这与定理 2.18 矛盾。

3.2　正约数的个数

定理 2.20　设整数 a 的标准分解式是

$a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}, p_1<p_2<\cdots<p_s, a_i>0, i=1,2,\cdots s$

那么 d 是 a 的正除数的充要条件是

$$d=p_1^{e_1}p_2^{e_2}\cdots p_s^{e_s}, 0\leqslant e_j\leqslant a_j, j=1,2,\cdots s。$$

证明:充分是显然的。下证必要性。

当 $d=1$ 时 $e_j=0, j=1,2,\cdots s$,结论成立。

若 $d>1$ 时,则由 $d|a$ 知 d 的素因数必在 $p_1,p_2,\cdots,p_s$ 中,所以 d 的标准分解式必为

$$d=p_1^{e_1}p_2^{e_2}\cdots p_s^{e_s}, 0\leqslant e_j, 1\leqslant j\leqslant s。$$

下证,$e_j\leqslant\alpha_j$,$(1\leqslant j\leqslant s)$,只证 $e_1\leqslant\alpha_1$ 即可,其它同理。

若 $e_1>\alpha_1$,则由 $d|a$ 推出,

$$p_1^{e_1-\alpha_1}p_2^{e_2}\cdots p_s^{e_s}\mid p_2^{\alpha_2}\cdots p_s^{\alpha_s}$$

所以,$p_1\mid p_2^{\alpha_2}\cdots p_s^{\alpha_s}$

所以 p_1 必与 $p_2,p_3,\cdots p_s$ 之一相等,矛盾。

推论 1　设 a,b 是正整数,且

$a=p_1^{\alpha_1}\cdots p_k^{\alpha_k}, b=p_1^{\beta_1}\cdots p_k^{\beta_k}, a_i,\beta_i\geqslant 0, i=1,2,\cdots,k$。

则 $(a,b)=p_1^{\gamma_1}\cdots p_k^{\gamma_k}$,$[a,b]=p_1^{\delta_1}p_2^{\delta_2}\cdots p_k^{\delta_k}$,

其中,$\gamma_i=\min\{\alpha_i,\beta_i\}$,$\delta_i=\max\{\alpha_i,\beta_i\}$,$i=1,2,\cdots,k$。

推论 2 若 $(a,b)=1$,$ab=c^k$,则 $a=u^k$,$b=\nu^k$。

证明:设 $c=p_1^{\alpha_1}\cdots p_s^{\alpha_s}$,$p_1<p_2<\cdots<p_s$ 是素数,$\alpha_j\geqslant 0$,$j=1,2,\cdots s$,则可设

$a=p_1^{\beta_1}\cdots p_s^{\beta_s}, b=p_1^{\gamma_1}\cdots p_s^{\gamma_s}, \beta_j\geqslant 0, \gamma_j\geqslant 0$,又 $ab=c^k$

所以,$\beta_j+\gamma_j=k\alpha_j$,$(1\leqslant j\leqslant s)$

由 $(a,b)=1$ 知 $\min\{\beta_i,\gamma_i\}=0$,$0\leqslant j\leqslant s$,则有

$\beta_j=0,\gamma_j=k\alpha_j$ 或 $\beta_j=k\alpha_j,\gamma_j=0$,则 $a=u^k$,$b=\nu^k$,显见 $u=(a,c)$,$\nu=(b,c)$。

定理 2.21　设 a 是正整数,$\tau(a)$ 表示 a 的所有正约数的个数(通常称 $\tau(a)$ 为约数函数)。

若 a 的标准素因数分解式 $a=p_1^{\alpha_1}\cdots,p_s^{\alpha_s}$,$p_1<p_2<\cdots<p_s$,

$\alpha_i>0, i=1,2,\cdots s$ 则

$\tau(a)=(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_s+1)=\tau(p_1^{\alpha_1})\tau(p_2^{\alpha_2})\cdots\tau(p_s^{\alpha_s})$。

证明：由定理 2.19 知 $d|a$ 的条件为

$d=p_1^{e_1}\cdots p_s^{e_s}$，其中 $0\leqslant e_i\leqslant\alpha_i, i=1,2,\cdots,s$。

而 e_i 有 α_i+1 种可能$(i=1,2,\cdots,s)$，故 d 有$(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_s+1)$个形式，即

$$\tau(a)=\tau(p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s})=\prod_{k=1}^{s}(\alpha_k+1)。$$

推论：若$(a,b)=1$，则 $\tau(ab)=\tau(a)\tau(b)$。

证明：设 a,b 的标准素因数分解式为 $a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$，$b=q_1^{\beta_1}q_2^{\beta_2}\cdots q_m^{\beta_m}$，由$(a,b)=1$ 知 $p_i\neq q_j, i=1,2,\cdots,n, j=1,2,\cdots,m$ 于是

$\tau(ab)=(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_n+1)(\beta_1+1)(\beta_2+1)\cdots(\beta_m+1)=\tau(a)\tau(b)$

此定理说明只要知道了正整数 a 的标准分解式，也就知道了它的所有的正约数，这一点有重要的应用价值。

例 1 设 n 是自然数，证明 $\varphi(n)\geqslant\frac{n}{\tau(n)}$，

其中 $\varphi(n)=n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_s}\right)$

证明：设 n 的标准素因数分解为 $n=p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$，则

$$\begin{aligned}\varphi(n)\tau(n)&=n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_r}\right)(k_1+1)\cdots(k_r+1)\\&\geqslant n\left(1-\frac{1}{2}\right)\left(1-\frac{1}{2}\right)\cdots\left(1-\frac{1}{2}\right)(1+1)\cdots(1+1)\\&=n\left(\frac{1}{2}\right)^r2^r\\&=n\end{aligned}$$

于是，$\varphi(n)\geqslant\frac{n}{\tau(n)}$。

例 2 试确定 $\tau(1)+\tau(2)+\cdots+\tau(1990)$的奇偶性。

解:设 n 的标准分解式为

$$n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k} \qquad (2)$$

其中 $p_1<p_2<\cdots<p_k, \alpha_i\geqslant 1, (i=1,2,\cdots k)$

则 $\tau(n)=(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_k+1)$,

由此可知若 $\tau(n)$为奇数,则 $\alpha_i, i=1,2,\cdots,k$ 都为偶数,

设 $\alpha_i=2\gamma_i, i=1,2,\cdots,k$,则

$n=(p_1^{\gamma_1}\cdots p_k^{\gamma_k})^2$,即 n 为完全平方数。若 n 为完全平方数,则 $\tau(n)$必为奇数。

由于,$45>\sqrt{1990}>44$

所以 1 至 1990 中有 44 个完全平方数,即在 $\tau(1),\tau(2),\cdots,\tau(1990)$中有 44 个奇数。

所以 $\tau(1)+\tau(2)+\cdots+\tau(1990)$为偶数。

例 3 设整数 a,b,c 大于 1,证明:

$$\frac{[a,b,c]^2}{[a,b][b,c][c,a]}=\frac{(a,b,c)^2}{(a,b)(b,c)(c,a)}$$

证明:设 a,b,c 的标准素数分解为:$a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}, b=p_1^{\beta_1}p_2^{\beta_2}\cdots p_n^{\beta_n}, c=p_1^{\gamma_1}\cdots p_n^{\gamma_n}$,其中 $\alpha_i,\beta_i,\gamma_i\geqslant 0, i=1,2,\cdots,n$。易证,

$$[a,b,c]^2=\prod_{i=1}^{n}p_i^{2\max\{\alpha_i,\beta_i,\gamma_i\}},$$

$$(a,b,c)^2=\prod_{i=1}^{n}p_i^{2\min\{\alpha_i,\beta_i,\gamma_i\}}。$$

不妨设,$\alpha_i\leqslant\beta_i\leqslant\gamma_i, i=1,2,\cdots,n$

于是

$$2\max\{\alpha_i,\beta_i,\gamma_i\}-\max\{\alpha_i,\beta_i\}-\max\{\beta_i,\gamma_i\}-\max\{\alpha_i,\gamma_i\}$$

$$=2\gamma_i-\beta_i-\gamma_i-\gamma_i=-\beta_i$$

$$2\min\{\alpha_i,\beta_i,\gamma_i\}-\min\{\alpha_i,\beta_i\}-\min\{\beta_i,\gamma_i\}-\min\{\alpha_i,\gamma_i\}$$

$$=2\alpha_i-\alpha_i-\beta_i-\alpha_i=-\beta_i$$

命题得证。

例 4 若 N 仅为 200…0 或 500…0 形的数，且 $\varphi(N)=2000$，求 N。

解：因为，$N=200\cdots0$ 或 $500\cdots0$

所以，$N=2^t5^{t-1}$ 或 $N=2^t5^{t+1}$

$\varphi(N)=2^t5^{t-1}\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)=2^{t+1}5^{t-2}$ 或 $\varphi(N)=2^t5^{t+1}\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)=2^{t+1}5^t$

又 $\varphi(N)=2000=2^45^3=2^{3+1}5^3$

$N=2^35^4=5000$。

3.3 正约数的和与积

定理 2.22 设 a 是正整数，$\sigma(a)$ 表示 a 的所有正约数之和。那么，$\sigma(1)=1$，当 a 有标准素因数分解数 $a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$ 时

$$\sigma(a)=\frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdots\frac{p_s^{\alpha_s+1}-1}{p_s-1}=\prod_{i=1}^{s}\frac{p_j^{\alpha_j+1}-1}{p_j-1}$$
$$=\sigma(p_1^{\alpha_1})\cdots\sigma(p_s^{\alpha_s}) \qquad (1)$$

证明 1：$\sigma(1)=1$ 显然。

当 $a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$ 时，把乘积

$(1+p_1+p_1^2+\cdots+p_1^{\alpha_1})$

$\times(1+p_2+p_2^2+\cdots+p_2^{\alpha_2})$

……

$\times(1+p_s+p_s^2+\cdots+p_s^{\alpha_1})$

展开，则共形成 $(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_s+1)=\tau(a)$ 项，其中每一项都是 $p_1^{x_1}p_2^{x_2}\cdots p_s^{x_s}$，$0\leqslant x_i\leqslant\alpha_i$，$i=1,2,\cdots,s$ 的形式，即每一项都是 a 的约数，且每个约数只出现一次，故可得(1)。

在采用第二种证法前，为了把证明叙述得更清楚，先引进几个有关求和与求积的符号，这在数学中经常用到。

设 h 是给定的整数，k 是给定的正整数。再设 Z_i 是依赖于参数 $i(h+1\leqslant i\leqslant h+k)$ 的 k 个复数。我们记 k 个复数和为

$$\sum_{i=h+1}^{h+k} Z_i = Z_{h+1} + \cdots + Z_{h+k} \tag{2}$$

它们的积为

$$\prod_{i=h+1}^{h+k} Z_i = Z_{h+1} \cdots Z_{h+k} \tag{3}$$

一般地，设 $h_1, \cdots, h_r$ 是给定的整数，$k_1, \cdots, k_r$ 是给定的正整数。再设 $Z_{i_1} \cdots, Z_{z_r}$ 是依赖于参数 $i_i(h_1+1 \leqslant i_1 \leqslant h_1+k_1), \cdots, i_r$ $(h_r+1 \leqslant i_r \leqslant h_r+k_r)$ 的 $k_1 \cdots k_r$ 个复数。我们以多重求和号

$$\sum_{\substack{h_j+1 \leqslant i_j \leqslant h_j+k_j \\ 1 \leqslant j \leqslant r}} Z_{i_1, i_2, \cdots i_r} \tag{4}$$

表示这 $k_1 \cdots k_r$ 个复数之和；以多重求积号

$$\prod_{\substack{h_j+1 \leqslant i_j \leqslant h_j+k_j \\ 1 \leqslant j \leqslant r}} Z_{i_1, \cdots, i_r} \tag{5}$$

表示这些复数之积。根据加法的交换律与结合律，多重和式(4)可表示为累次求和：

$$\begin{aligned} &\sum_{h_j+1 \leqslant i_j \leqslant h_j+k_j} Z_{i_1, i_2 \cdots, i_r} \\ &= \sum_{i_1=h_1+1}^{h_1+k_1} \cdots \sum_{i_{r-1}=h_{r-1}+1}^{h_{r-1}+k_{r-1}} \sum_{i_r=h_r}^{h_r+k_r} Z_{i_1, \cdots, i_{r-1}, i_r} \end{aligned} \tag{6}$$

上式右边的累次求和式是表示：对固定的 $i_1, \cdots, i_{r-1}$，先对参数 $i_r(h_r+1 \leqslant i_r \leqslant h_r+k_r)$ 给出的 k_r 个复数 $Z_{i_1, \cdots, i_{r-1}, i_r}$ 求和得到 $Z^{(1)}_{i_1, \cdots, i_{r-1}}$，这是依赖于参数 $i_1(h_1+1 \leqslant i_1 \leqslant h_1+k_1), \cdots, i_{r-1}$ $(h_{r-1}+1 \leqslant i_{r-1} \leqslant h_{r-1}+k_{r-1}$ 的复数；再固定 $i_1, \cdots, i_{r-2}$，先对参数 $i_{r-1}(h_{r-1}+1 \leqslant i_{r-1} \leqslant h_{r-1}+k_{r-1})$ 给出的 k_{r-1} 个复数 $Z^{(1)}_{i_1, \cdots, i_{r-1}}$ 求和得到 $Z^{(2)}_{i_1, \cdots, i_{r-2}}$，等等，通过这样的求和次序来求出多重和式(4)。通常，把这种累次求和称为是先对参数 i_r 求和，再对 i_{r-1} 求和，…，最后对参数 i_1 求和。显然，由加法的交换律和结合律知，这种对参数 $i_1, \cdots, i_r$ 的累次求和的次序可以任意选定。同样，根据乘法的交换律与结合律，多重乘积(5)可表达为累次求积

$$\prod_{\substack{h_j+1\leqslant i_j\leqslant h_j+k_j\\1\leqslant j\leqslant r}} Z_{i_1,\cdots,i_r}$$

$$=\prod_{i_1=h_1+1}^{h_1+k_1}\cdots\prod_{i_{r-1}=h_{r-1}+1}^{h_{r-1}+k_{r-1}}\prod_{i_r=h_r+1}^{h_r+k_r} Z_{i_1,\cdots,i_{r-1},i_r} \qquad (7)$$

累次求积的意义和累次求和完全一样。

设 f(d)是定义在全体正整数集合上的复值函数,a 是给定的正整数。在数论中经常用以下的符号:

$\sum\limits_{d|a}f(d)$ = 函数 f 在 a 的所有不同的正除数上的值之和; (8)

$\sum\limits_{p|a}f(p)$ = 函数 f 在 a 的所有不同的素除数上的值之和; (9)

$\prod\limits_{d|a}f(d)=\prod\limits_{p|a}f(p)=f(n)\equiv 1\tau(a)=\sum\limits_{d|a}1f(n)=n\sigma(a)=\sum\limits_{d|a}df(n)$

引理　设 $f(n)$是定义在正整数集合上的复值函数,正整数 a 同定理 2.22 中的 a,那么

$$\sum_{d|a}f(d)=\sum_{e_1=0}^{a_1}\cdots\sum_{e_s=0}^{a_s}f(p_1^{e_1}\cdots p_s^{e_s})$$

$$\prod_{d|a}f(d)=\prod_{e_1=0}^{a_1}\cdots\prod_{e_s=0}^{a_s}f(p_1^{e_1}\cdots p_s^{e_s})e_1,\cdots,e_s$$

$$\begin{cases}Z_{e_1,\cdots,e_s}=f(p_1^{e_1}\cdots p_s^{e_s})\\(-1)+1=0\leqslant e_j\leqslant a_j=(-1)+a_j+1,1\leqslant j\leqslant s,\end{cases}$$

定理 2.22 的证明 Ⅱ

$$\sigma(a)=\sum_{e_1=0}^{a_1}\cdots\sum_{e_s=0}^{a_s}p_1^{e_1}\cdots p_s^{e_s}$$

$$=\sum_{e_1=0}^{a_1}\cdots\sum_{e_{s-1}=0}^{a_{s-1}}p_1^{e_1}\cdots p_{s-1}^{e_{s-1}}(\sum_{e_s=0}^{a_s}p_s^{e_s})$$

$$=(\sum_{e_s=0}^{a_s}p_s^{e_s})\cdot(\sum_{e_1=0}^{a_1}\cdots\sum_{e_{s-1}=0}^{a_{s-1}}p_1^{e_1}\cdots p_{s-1}^{e_{s-1}})$$

继续对上式右边的累次求和用以上的推导,最后就得

$$\sigma(a)=(\sum_{e_1=0}^{a_1}p_1^{e_1})\cdots(\sum_{e_s=0}^{a_s}p_s^{e_s})=\sigma(p_1^{a_1})\cdots\sigma(p_s^{a_s})a。$$

推论：或$(a,b)=1$，则 $\sigma(ab)=\sigma(a)\sigma(b)$

证明略

例 1 证明：正整数 n 的所有正约数的乘积 p 等于 $n^{\frac{\tau(n)}{2}}$，其中 $\tau(n)$表示 n 的正约数的个数。

证明：因为 n 的所有正约数的个数是 $\tau(n)$，所以设它们为 $d_1,d_2,\cdots,d_{\tau(n)}$。显然$\frac{n}{d_1},\frac{n}{d_2},\cdots,\frac{n}{d_{\tau(n)}}$也是 n 的 $\tau(n)$个正约数，于是有 $p=d_1\cdot d_2\cdot\cdots\cdot d_{\tau(n)}=\frac{n}{d_1}\cdot\frac{n}{d_2}\cdots\frac{n}{d_{\tau(n)}}=\frac{n^{\tau(n)}}{p}$。

即 $p^2=n^{\tau(n)}$，从而有 $p=n^{\frac{\tau(n)}{2}}$。

定义 2.5 若 $\sigma(a)=2a$，则 a 叫做**完全数**。

例如 $\sigma(6)=1+2+3+6=2\times6$，

$\sigma(28)=\sigma(2^2\cdot7)=\frac{2^3-1}{2-1}\cdot\frac{7^2-1}{7-1}=7\times8=2\times28$。

例 2 求证，若 2^n-1 为素数，则 $2^{n-1}(2^{n-1})$为完全数，并且无其它偶完全数。

证明：(1) 令 $p=2^n-1$，则

$\sigma(2^{n-1}(2^n-1))=\sigma(2^{n-1}p)=\frac{2^n-1}{2-1}\cdot\frac{p^2-1}{p-1}=(p+1)(2^n-1)=2\cdot2^{n-1}(2^n-1)$

所以，$2^{n-1}(2^n-1)$为完全数。

(2) 若 a 为偶完全数，令 $a=2^{n-1}u$，$n>1$，$2\nmid u$，则

$$2^nu=2a=\sigma(a)=\sigma(2^{n-1})\sigma(u)=\frac{2^n-1}{2-1}\sigma(u)$$

即 $\sigma(u)=\frac{2^nu}{2^n-1}=u+\frac{u}{2^n-1}$

此式代表 u 的约数和为两个数之和，故 u 为素数，且$\frac{u}{2^n-1}=1$，即 $u=2^n-1$，所以 $a=2^{n-1}(2^n-1)$。

例 3 求证若一正整数为其真约数之积，则此数必为一素数

之立方或两不同素数之积,且无其它正整数具有此性质。

证明:设 a 为其真约数之积,

则 $a^2=\prod\limits_{d|a}\mathrm{d}=\prod\limits_{d|a}\frac{\mathrm{a}}{\mathrm{d}}$,

则 $a^4=\prod\limits_{d|a}\mathrm{d}\prod\limits_{d|a}\frac{\mathrm{a}}{\mathrm{d}}=\prod\limits_{d|a}\left(\mathrm{d}\cdot\frac{\mathrm{a}}{\mathrm{d}}\right)=\prod\limits_{d|a}\mathrm{a}=a^{\tau(a)}$,

所以 $\tau(a)=4$。

令 $a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$,则$(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_s+1)=4$。

若 $s=1$,则 $\alpha_1=3$,即 $a=p_1^3$;

若 $s=2$,则 $\alpha_1=\alpha_2=1$,即 $a=p_1p_2$;

若 $s\geqslant3$,$\tau(a)\geqslant8$,故必有

$a=p_1^3$,或 $a=p_1p_2$。

第三章　竞赛中的几个典型问题

§1　高斯函数$[x]$、$\{x\}$

$[x]$和$\{x\}$是非常重要的数论函数,其他许多数学分支都要涉及到,在国内外的数学竞赛中也经常出现含有$[x]$及$\{x\}$的问题,这类问题新颖独特,颇具启发性。要解决涉及$[x]$及$\{x\}$的问题,需要掌握有关的基本知识和技能,系统地学习这方面的知识。

定义 3.1　设 $x\in R$,不超过 x 的最大整数称为高斯函数,记为$[x]$。

显然$[x]$是整数,且满足 $x-1<[x]\leqslant x<[x]+1$。函数 $y=[x]$的定义域为 R,值域是整数集 Z。

例如$[3\cdot 2]=3$,$[-3\cdot 2]=-4$,$[3]=3$,$[-4]=-4$。

定义 3.2　称 $x-[x]$为 x 的小数部分或分数部分,记为$\{x\}$

显然 $0\leqslant\{x\}<1$,例如$\{-1.2\}=0.8$,$\{1.2\}=0.2$,$\{3\}=0$

$y=\{x\}$的定义域为 R,值域为$[0,1)$。

任一实数都能写成整数部分与非负纯小数之和,即 $x=[x]+\{x\}$。

函数 $y=[x]$及 $y=\{x\}$的图像见图 3.1 和图 3.2。

§2　基本性质

定理 3.1　设 x,y 是实数,有

(1) 若 $x\leqslant y$ 则$[x]\leqslant[y]$,即 $y=[x]$是不减函数

(2) 任意整数 m,$[x+m]=[x]+m$,$\{x+m\}=\{x\}$,$\{x\}$是周期为 1 的周期函数。

(3) $[x]+[y]\leqslant[x+y]\leqslant[x]+[y]+1$,其中等号有且仅有

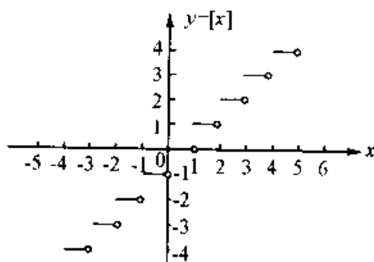


图 3.1

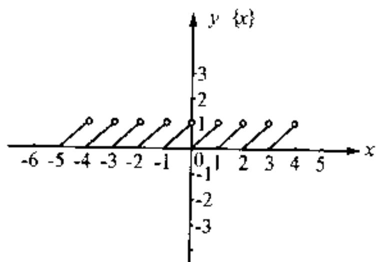


图 3.2

一个成立。$\{x+y\}\leqslant\{x\}+\{y\}$

(4) $[-x]=\begin{cases}-[x] & x\in Z\\ -[x]-1 & x\notin Z\end{cases}$

及 $\{-x\}=\begin{cases}-\{x\}=0 & x\in Z\\ 1-\{x\} & x\notin Z\end{cases}$

证明 (1)由 $[x]\leqslant x\leqslant y<[y]+1$ 即得

(2)由 $[x]+m\leqslant x+m<([x]+m)+1$ 即得

(3) $x+y=[x]+[y]+\{x\}+\{y\}$ $0\leqslant\{x\}+\{y\}<2$

当 $0\leqslant\{x\}+\{y\}<1$ 时,知 $[x+y]=[x]+[y]$

当 $1\leqslant\{x\}+\{y\}<2$ 时, $[x+y]=[x]+[y]+[\{x\}+\{y\}]=[x]+[y]+1$

由此有 $[x]+[y]\leqslant[x+y]\leqslant[x]+[y]+1$

$\{x+y\}=x+y-[x+y]\leqslant x+y-[x]-[y]=\{x\}+\{y\}$

即 $\{x+y\}\leqslant\{x\}+\{y\}$

(4) $x\in Z$ 时显然。x 不是整数时, $-x=-[x]-\{x\}=-[x]-1+1-\{x\}$

$0<1-\{x\}<1$,命题得证。

定理 3.2 对正整数 m 有 $\left[\frac{[x]}{m}\right]=\left[\frac{x}{m}\right], x\in R$

证明:由带余除法知,存在整数 q, r,使得 $[x]=qm+r$,其中

$0\leqslant r<m$，即$\frac{[x]}{m}=q+\frac{r}{m}\quad 0\leqslant\frac{r}{m}<1$

故$\left[\frac{[x]}{m}\right]=q$，又$\frac{x}{m}=\frac{[x]+\{x\}}{m}=\frac{[x]}{m}+\frac{\{x\}}{m}=q+\frac{r+\{x\}}{m}$，

由于$0\leqslant\frac{r+\{x\}}{m}<1$

故$\left[\frac{x}{m}\right]=q$，即$\left[\frac{[x]}{m}\right]=\left[\frac{x}{m}\right]$

定理 3.3　$x\in R^{+}$，$n\in N$，则 1 至 x 之间的整数中，有$\left[\frac{x}{n}\right]$个是 n 的倍数。

证明：因$\left[\frac{x}{n}\right]\leqslant\frac{x}{n}<\left[\frac{x}{n}\right]+1$，即$\left[\frac{x}{n}\right]\cdot n\leqslant x<\left(\left[\frac{x}{n}\right]+1\right)n$

这说明不大于 x 而是 n 的倍数的正整数只有下列$\left[\frac{x}{n}\right]$个：

$$n,2n\cdots\cdots\left[\frac{x}{n}\right]\cdot n$$

例如　100～500 中是 11 的整数倍的数有$\left[\frac{500}{11}\right]-\left[\frac{100}{11}\right]=$ 36 个。

例 1　求$\left[\frac{305\times1}{503}\right]+\left[\frac{305\times2}{503}\right]+\cdots+\left[\frac{305\times501}{503}\right]+\cdots+\left[\frac{305\times502}{503}\right]$的值。

解：$x+y=[x]+[y]+\{x\}+\{y\}$，若$\{x\}+\{y\}=1$，则$[x+y]=[x]+[y]+1$，由于 503 是素数，故当 $n=1,2\cdots502$ 时，$\frac{305n}{503}$不是整数，又$\frac{305n}{503}+\frac{305(503-n)}{503}=305$，故$\left\{\frac{305n}{503}\right\}+\left\{\frac{305(503-n)}{503}\right\}=1$。

则　$\left[\frac{350n}{503}\right]+\left[\frac{305(503-n)}{503}\right]=305-1=304$

将题中的 502 项两两配对，即得

$\sum_{n=1}^{502}\left[\frac{305n}{503}\right]=304\times\frac{502}{2}=76304$.

例 2 证明$[x]+[2x]+[4x]+[8x]+[16x]+[32x]=12345$无实数解。

证明：设 $x=[x]+\{x\}$，令$[x]=N$，$\{x\}=\alpha$，$0\leqslant\alpha<1$

$[x]=N$，$[2x]=[2n+2\alpha]=2N+[2\alpha]$，$[4x]=4N+[4\alpha]$，$[8x]=8N+[8\alpha]$，$[16x]=16N+[16\alpha]$，$[32x]=32N+[32\alpha]$故原方程变为$[2\alpha]+[4\alpha]+[8\alpha]+[16\alpha]+[32\alpha]=12345-63N$

由于$0\leqslant\alpha<1$，故$0\leqslant2\alpha<2$，$0\leqslant4\alpha<4$，$0\leqslant8\alpha<8$，$0\leqslant16\alpha<16$，$0\leqslant32\alpha<32$，故有$0\leqslant12345-63N<1+3+7+15+31=51$

即得$195.0476\leqslant N\leqslant195.95238$，而 $N=[x]$是整数，故原方程无实数解。

例 3 证明当 $n=1,2\cdots$时，$[(1+\sqrt{2})^n]$交错地取偶数与奇数值。

证明：由$(1+\sqrt{2})^n+(1-\sqrt{2})^n=2[1+(\sqrt{2})^2C_n^2+(\sqrt{2})^4C_n^4+(\sqrt{2})^6C_n^6+\cdots\cdots+(\sqrt{2})^kC_n^k]$，$k=\begin{cases}n & n\text{ 为偶数}\\ n-1 & n\text{ 为奇数}\end{cases}$

又$-1<1-\sqrt{2}<0$，故$[(1+\sqrt{2})]^n+[(1-\sqrt{2})^n]=(1+\sqrt{2})^n+(1-\sqrt{2})^n-1$。

则 $$[(1+\sqrt{2})^n]=\begin{cases}(1+\sqrt{2})^n+(1-\sqrt{2})^n-1 & \text{若 } n \text{ 为偶数}\\ (1+\sqrt{2})^n+(1-\sqrt{2})^n & \text{若 } n \text{ 为奇数}\end{cases}$$

从而$[(1+\sqrt{2})^n]$交错地取偶数与奇数值。

例 4 求方程$4x^2-40[x]+51=0$的全部实根。

解：由$4x^2=40[x]-51$是奇数，可设$4x^2=2k+1$　$k\in Z^+$

于是 $x=\pm\sqrt{\frac{2k+1}{4}}$（负根不合题意，舍掉）故 $x=\frac{1}{2}\sqrt{2k+1}$

原方程化成：$\left[\frac{1}{2}\sqrt{2k+1}\right]=\frac{k+26}{20}$，由于左端是整数，则

$\frac{k+26}{20}$是整数，$k=20t+14 \quad (t=0,1,2\cdots)$

另一方面又有$\frac{k+20}{20}<\frac{1}{2}\sqrt{2k+1}<\frac{k+20}{20}+1$

解此不等式可得 $4\leqslant k<24$ 或 $84<k\leqslant 144$，其中满足 $k=20t+14$ 的有 14,94,114,134，对应的解分别是

$$x_1=\frac{\sqrt{29}}{2}, x_2=\frac{\sqrt{189}}{2}, x_3=\frac{\sqrt{229}}{2}, x_4=\frac{\sqrt{269}}{2}$$

例 5 设 M 为一正整数，求方程 $x^2-[x^2]=(x-[x])^2$ 在 $[1,M)$ 中解的个数。

解 显然 $x=M$ 是一个解。下考察在$[1,M)$中有多少个解。

设 x 是方程的解，得 $x=[x]+\{x\}$代人原方程并化简得 $2[x]\{x\}=[2[x]\{x\}+\{x\}^2]$。由于 $0\leqslant\{x\}<1$，则此方程有解当且仅当 $2[x]\{x\}$是整数 k。

设$[x]=m$，则$\{x\}=\frac{k}{2m}$ $(k=0,1,\cdots,2m-1)$，即在$[m,m+1)$中方程有 $2m$ 个解，又由于 $1\leqslant m\leqslant m-1$，可知在$[1,M)$中方程有 $2(1+2+\cdots+M-1)=M(M-1)$个解。原方程在$[1,M)$中有 $M(M-1)$个解。

例 6 设 $1<a<2$，k 为一整数，求证

$$\left[a\left[\frac{k}{2-a}\right]+\frac{a}{2}\right]=\left[\frac{ak}{2-a}\right]$$

证明：设 $n=\left[\frac{k}{2-a}\right]$，$\frac{k}{2-a}=n+x$，$0\leqslant x<1$

由 $1<a<2$ 知 $0<\frac{k}{n+x}=2-a<1$，故 $a=2-\frac{k}{n+x}$，$\frac{a}{2}=1-\frac{k}{2(n+x)}$

故原式左端$=\left[\left(2-\frac{k}{n+x}\right)n+1-\frac{k}{2(n+x)}\right]=2n-k+1+\left[\frac{\left(x-\frac{1}{2}\right)k}{n+x}\right]$

原式右端$=\left[\left(2-\frac{k}{n+x}\right)(n+x)\right]=2n-k+[2x]$

当$0\leqslant x<\frac{1}{2}$时,左端$=2n-k=$右端

当$\frac{1}{2}\leqslant x<1$时,$[2x]=1$,左端$=2n-k+1$,右端$=2n-k+1$。命题得证。

定理 3.4 (埃尔米特 *Hermite* 恒等式)$x\in R,n\in N$,则$[x]+\left[x+\frac{1}{n}\right]+\left[x+\frac{2}{n}\right]+\cdots+\left[x+\frac{n-1}{n}\right]=[nx]$

证明:(1) 引入辅助函数 $f(x)=[nx]-[x]-\left[x+\frac{1}{n}\right]-\left[x+\frac{2}{n}\right]\cdots\cdots-\left[x+\frac{n-1}{n}\right]$

因为 $f\left(x+\frac{1}{n}\right)=[nx+1]-\left[x+\frac{1}{n}\right]-\left[x+\frac{2}{n}\right],\cdots\cdots,-[x+1]=f(x)$对一切 $x\in R$ 成立,故 $f(x)$是以$\frac{1}{n}$为周期的周期函数。当 $x\in\left[0,\frac{1}{n}\right]$时,$f(x)=0$ 故对任意 $x\in R$,埃尔米特恒等式成立。

(2) 设 $x=[x]+\{x\}$则原式等价于

$[\{x\}]+\left[\{x\}+\frac{1}{n}\right]+\cdots+\left[\{x\}+\frac{n-1}{n}\right]=[n\{x\}]$,与原等式相同。因此只需证原式对 $x\in[0,1)$成立即可。

把$[0,1)$分成几个小区间$\left\{\left[0,\frac{1}{n}\right),\left[\frac{1}{n},\frac{2}{n}\right),\cdots\left[\frac{n-1}{n},1\right)\right\}$由于 $x\in[0,1)$,则一定存在 k 使得$\frac{k-1}{n}\leqslant x<\frac{k}{n}$,即 $k-1\leqslant nx<k$

故原式右端$=[nx]=k-1$,又由$\frac{k}{n}\leqslant x+\frac{1}{n}<\frac{k+1}{n}$,$\frac{k+1}{n}\leqslant x+\frac{2}{n}<\frac{k+2}{n},\cdots,\frac{k+i}{n}\leqslant x+\frac{i+1}{n}<\frac{k+i+1}{n},\cdots\frac{k+n-2}{n}\leqslant x+\frac{n-1}{n}<\frac{k+n-1}{n}$,上述不等式的右端总有一个等于 1,设$\frac{k+t}{n}=$

1,即 $t=n-k$,这时有

$$[x]=\left[x+\frac{1}{n}\right]=\cdots\left[x+\frac{t}{n}\right]=0$$

$$\left[x+\frac{n-k+1}{n}\right]=\left[x+\frac{n-k+2}{n}\right]=\cdots=\left[x+\frac{n-1}{n}\right]=1$$

故原式的左边是 $k-1$ 个 1 之和,即左 $=k-1=$ 右,由此命题得证。

(3) 设 $[nx]=qn+r \quad q\in Z, 0\leqslant r<n$,下证 $\sum_{i=0}^{n-1}\left[x+\frac{i}{n}\right]=nq+r$

由 $[nx]=nq+r$ 易知 $nq+r\leqslant nx<nq+r+1$

$$q+\frac{r}{n}\leqslant x<q+\frac{r+1}{n}$$

$$q+\frac{r+i}{n}\leqslant x+\frac{i}{n}<q+\frac{r+i+1}{n}$$

因此有 $\left[x+\frac{i}{n}\right]=q+\left[\frac{r+i}{n}\right] \quad i=0,1,\cdots n-1$,设 $r=n-k$,$n\geqslant k>0$,则要使 $r+i\geqslant n$,必有 $k\leqslant i\leqslant n-1$

$\sum_{i=0}^{n-1}\left[x+\frac{i}{n}\right]=nq+\sum_{i=0}^{n-1}\left[\frac{r+i}{n}\right]=nq+\sum_{i=k}^{n-1}\left[\frac{r+i}{n}\right]=nq+r$,故命题得证。

例 7 对任意 $n\in N$,计算 $S=\sum_{k=0}^{\infty}\left[\frac{n+2^k}{2^{k+1}}\right]$

解:$\left[\frac{n+2^k}{2^{k+1}}\right]=\left[\frac{1}{2}+\frac{n}{2^{k+1}}\right]$,由 *Hermite* 恒等式可得

$\left[\frac{n}{2^{k+1}}+\frac{1}{2}\right]=\left[2\cdot\frac{n}{2^{k+1}}\right]-\left[\frac{n}{2^{k+1}}\right]$,又由于 n 固定,当 k 充分大时,$\frac{n}{2^k}<1$,即当 $k>[\log_2 n]$ 时,$\left[\frac{n}{2^k}\right]=0$,故

$S=\sum_{k=0}^{\infty}\left(\left[\frac{n}{2^k}\right]-\left[\frac{n}{2^{k+1}}\right]\right)=[n]-\left[\frac{n}{2}\right]+\left[\frac{n}{2}\right]-\left[\frac{n}{2^2}\right]+\cdots$
$\left[\frac{n}{2^{\log_2 n}}\right]-\left[\frac{n}{2^{\log_2 n+1}}\right]=n$

即 $S=\sum_{k=0}^{\infty}\left[\frac{n+2^{k}}{2^{k+1}}\right]=n$

定理 3.5 平面上坐标为整数的点称为整点或格点。设 $x_1<x_2$ 是实数，$y=f(x)$ $(x_1<x\leqslant x_2)$是非负连续函数。证明：

(1) 区域 $x_1<x\leqslant x_2, 0<y\leqslant f(x)$上整点的个数

$$M=\sum_{x_1<n\leqslant x_2}[f(n)], n\in Z$$

(2) $[x_1]-[x_2]<M-\sum_{x_1<n\leqslant x_2}f(n)\leqslant 0$

证明：(1)所说区域上的整点，都在这样的直线段上：$x=n$，$1\leqslant y\leqslant f(n)$，$n$、$y\in Z$，$x_1<n\leqslant x_2$，而 y 的个数就是$[f(n)]$，故 $M=\sum_{x_1<n\leqslant x_2}f(n)$。参见图 3.3

(2) 由 $\sum_{x_1<n\leqslant x_2}[f(n)]=\sum_{x_1<n\leqslant x_2}f(n)-\sum_{x_1<n\leqslant x_2}\{f(n)\}$

$0\leqslant\sum_{x_1<n\leqslant x_2}\{f(n)\}<\sum_{x_1<n\leqslant x_2}1$

$\sum_{x_1<n\leqslant x_2}1-\sum_{[x_1]+1\leqslant n\leqslant[x_2]}1=[x_2]-[x_1]$ 这三式可知

$$[x_1]-[x_2]<M-\sum_{x_1<n\leqslant x_2}f(n)\leqslant 0$$

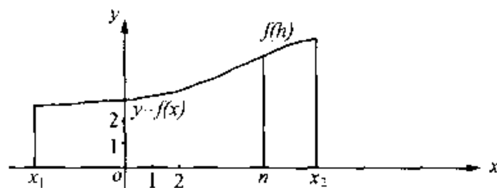


图 3.3

定义 3.3 设 p 是一给定的素数，如果对正整数 n 有 $p^m\mid n$，而 $p^{m+1}\nmid n$，m 为非负整数，则记 $p(n)=m$，如 $2(7)=0$，$2(24)=3$。即 m 是表示 p 在 n 中的最高幂。

对于有理数$\frac{a}{b}$，定义 $p\left(\frac{a}{b}\right)=p(a)-p(b)$

$p(n)$有以下两条简单性质。

(1) $p(mn)=p(m)+p(n)$ $\quad m, n\in N$

(2) $p(n^k)=kp(n) \qquad k\in N$

如果我们知道了每一个素数 p 的 $p(n)$ 值,那么就可以十分容易地将 n 分解为素数的乘积。但是要实现这一点是比较困难的,目前只对 $p(n!)$ 有一些结论。

定理 3.6 设 p 是素数,$n\in N$,且 $p^k\leqslant n<p^{k+1}$,则

$$p(n!)=\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\cdots+\left[\frac{n}{p^k}\right]$$

证明:

由于 p 是素数,所以 $n!$ 中 p 的方次数是 $1,2\cdots n$ 中各数 p 的方次数之总和。由定理 3.3 知,$1,2\cdots n$ 中有 $\left[\frac{n}{p}\right]$ 个 p 的倍数,有 $\left[\frac{n}{p^2}\right]$ 个 p^2 的倍数……设 $p^k\leqslant n<p^{k+1}$,则 $\left[\frac{n}{p^{n+1}}\right]=\left[\frac{n}{p^{k+2}}\right]=\cdots=0$,故 $n!$ 中 p 的方次数为:

$$p(n!)=\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\cdots+\left[\frac{n}{p^k}\right]=\sum_{t=1}^{k}\left[\frac{n}{p^t}\right]$$

定理 3.6 中的结论也常写成下面形式,$p(n!)=\sum_{t=1}^{\infty}\left[\frac{n}{p^t}\right]$

推论:$n!$ 的素数分解式为 $n!=\prod_{p<n}p^{\sum_{t=1}^{\infty}\left[\frac{n}{p^t}\right]}$,$p$ 为素数。

例 8 证明有无穷多个正整数 m,满足 $m-2(m!)=2000$。

证明:将 m 用二进制表示:$m=\sum_j 2^{r_j}=2^{r_n}+2^{r_{n-1}}+\cdots+2^{r_1}$

其中整数 $r_n>r_{n-1}>\cdots>r_1\geqslant 0$,由定理 3.6 得

$2(m!)=\left[\frac{m}{2}\right]+\left[\frac{m}{2^2}\right]+\cdots=\sum_j 2^{r_j-1}+\sum_j 2^{r_j-2}+\sum_j 2^{r_j-3}+\cdots$
$(r_j-t\geqslant 0,t=1,2,3\cdots)=\sum_j(2^{r_j-1}+2^{r_j-2}+\cdots+1)=\sum_j(2^{r_j}-1)$
$=m-n$。

故 $m-2(m!)=n$,即 $m-2(m!)$ 等于 m 在二进制中非零数字的个数,有无穷多个 m 的二进制表示中恰有 2000 个非零数字。

例 9 求自然数 1998! 末尾零的个数。

解：$5(1998!)=\left[\frac{1998}{5}\right]+\left[\frac{1998}{5^2}\right]+\left[\frac{1998}{5^3}\right]+\left[\frac{1998}{5^4}\right]=399+79+15+3=496$

又显然 $2(1998!)>5(1998!)$

故 1998! 末尾零的个数为 496 个

例 10 求圆 $x^2+y^2=r^2$ 内的整点个数。

解：用 T_1,T_2,T_3,T_4 分别表示如下区域上的整点数：

$T_1: x=0, 0<y\leqslant r$ $T_2: 0<x\leqslant\frac{\sqrt{2}}{2}r, \frac{\sqrt{2}}{2}r<y\leqslant\sqrt{r^2-x^2}$

$T_3: 0<y\leqslant\frac{\sqrt{2}}{2}r, \frac{\sqrt{2}}{2}r<x\leqslant\sqrt{r^2-y^2}$ $T_4: 0<x\leqslant\frac{\sqrt{2}}{2}r, 0<y\leqslant\frac{r}{\sqrt{2}}$

由圆的性质知 $T_3=T_2$

$$T_1=[r], T_3=\sum_{0<x\leqslant\frac{\sqrt{2}}{2}r}\left[\sqrt{r^2-x^2}\right]-T_4,$$

$$T_2+T_4=\sum_{0<x\leqslant\frac{\sqrt{2}}{2}r}\left[\sqrt{r^2-x^2}\right]$$

$T_4=\left[\frac{\sqrt{2}}{2}r\right]^2$，原点也是一个整点，故圆域上的整点个数为：

$$1+4(T_1+T_2+T_3+T_4)=1+4[r]+8\sum_{0<x\leqslant\frac{\sqrt{2}}{2}r}\left[\sqrt{r^2-x^2}\right]-4\left[\frac{\sqrt{2}}{2}r\right]^2$$

例 11 设 a 和 b 是整数，$n\in N$，求证：

$$\frac{b^{n-1}a(a+b)(a+2b)\cdots(a+(n-1)b)}{n!}\text{是整数}$$

证明：设 p 是不大于 n 的质数，则 $p\geqslant 2$，且

$$p(n!)=\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\cdots<\frac{n}{2}+\frac{n}{2^2}+\cdots=n$$

(1) 如果 $p\mid b$，显然命题成立。

(2) $p\nmid b$，由 p 个数 $a, a+b, a+2b\cdots a+(p-1)b$ 中至少有一个能被 p 整除，且 $p\leqslant n$，则在 n 个数的乘积 $a(a+b)(a+2b)$

$\cdots(a+(n-1)b)$中至少有$\left[\frac{n}{p}\right]$个数能被p整除,至少有$\left[\frac{n}{p^2}\right]$个数能被$p^2$整数……所以$p$在$a(a+b)\cdots(a(n-1)b)$中的方次数不小于$p(n!)$,于是分母中$p$的约数可以约去。由$p$的任意性,命题得证。

§3 技巧与方法

高斯函数是一个非常重要的数论函数,其应用非常广泛。在数学竞赛中经常出现关于$[x]$的方程,等式,不等式,整除问题,格点问题,组合数问题以及二项式定理问题等,内容非常丰富,技巧十分巧妙。在解这类题目时,一定要熟悉前面介绍的基本性质及定理。并灵活运用。这类题目大都无常规可解题方法,只有通过大量的练习,才能熟能生巧,掌握这类题的解决方法。下面再介绍几道典型的题目。

例 1 求$[(\sqrt{29}+\sqrt{21})^{2000}]$的末两位数字。

解:令 $\alpha=\sqrt{29}+\sqrt{21},\quad \beta=\sqrt{29}-\sqrt{21}$

则 $\alpha^2=50+2\sqrt{609},\quad \beta^2=50-2\sqrt{609}$

则 $\alpha^2+\beta^2=100, \alpha^2\cdot\beta^2=64$ 令 $a=\alpha^2, b=\beta^2$,则 a,b 是方程 $x^2-100x+64=0$ 的两根。

令 $S_0=a^0+b^0=2, S_1=a+b$

$S_2=a^2+b^2$,则 $S_2-100S_1+64S_0=0$

$S_3=a^3+b^3$,则 $S_3-100S_2+64S_1=0$

$\vdots$

$\vdots$

$S_n=a^n+b^n$,则 $S_n-100S_{n-1}+64S_{n-2}=0$

则 $\quad S_n\equiv-64S_{n-2}\equiv36S_{n-2}(\mathrm{mod}100)$

$n=1000$ 时,$S_n\equiv36(a^{998}+b^{998})\equiv36^{499}(a^0+b^0)\equiv2\times6^{499}(\mathrm{mod}100)$

即 $\alpha^{2000}+\beta^{2000}\equiv2\times6^{499}\equiv32(\mathrm{mod}100)$

即　　$(\sqrt{29}+\sqrt{21})^{2000}+(\sqrt{29}-\sqrt{21})^{2000}$的末两位数是32。

又　　$0<\sqrt{29}-\sqrt{21}<1, 0<(\sqrt{29}-\sqrt{21})^{2000}<1$

故　　$[(\sqrt{29}+\sqrt{21})^{2000}]=S_n-1=S_{1000}-1$,

即　　$[(\sqrt{29}+\sqrt{21})^{2000}]$的末两位数是31。

当遇到$(a\sqrt{p}+b\sqrt{q})^n$形式时,往往与$(a\sqrt{p}-b\sqrt{q})^n$同时考虑,由此可以化为整数。主要利用以下几条性质:

(1) $(a\pm b)^n=a^n+C_n^1a^{n-1}(\pm b)+\cdots+(\pm b)^n$

(2) $(a+b)^n+(a-b)^n=2(a^n+C_n^2a^{n-2}b^2+\cdots+C_n^ka^{n-k}b^k)$

其中 $k=\begin{cases} n & n\text{ 为偶数} \\ n-1 & n\text{ 为奇数} \end{cases}$

(3) 若$\{x\}+\{y\}=1$,则$[x]+[y]=[x+y]-1$

例2　前1000个自然数中,有多少个数可以写成$[2x]+[4x]+[6x]+[8x]$的形式,其中$x\in R$。

解:令$f(x)=[2x]+[4x]+[6x]+[8x]$,则$f(x+\frac{1}{2})=f(x)+10$

由此只需考虑$x\in\left[0,\frac{1}{2}\right)$时,$f(x)$能表达哪些自然数,当$x\in\left[0,\frac{1}{2}\right)$时,$[2x]=0$, $f(x)=[4x]+[6x]+[8x]$.

(1) 当$x\in\left[0,\frac{1}{8}\right)$时,$f(x)=0$

(2) 当$x\in\left[\frac{1}{8},\frac{1}{6}\right)$时,$f(x)=1$

(3) 当$x\in\left[\frac{1}{6},\frac{1}{4}\right)$时,$f(x)=1+1=2$

(4) 当$x\in\left[\frac{1}{4},\frac{1}{3}\right)$时,$f(x)=4$

(5) 当$x\in\left[\frac{1}{3},\frac{3}{8}\right)$时,$f(x)=5$

(6) 当 $x\in\left[\frac{3}{8},\frac{1}{2}\right)$时，$f(x)=6$

$f\left(\frac{1}{2}\right)=10$，即当 $x\in\left[0,\frac{1}{2}\right]$时，$f(x)$可以表示 1,2,4,5,6,10 这 6 个自然数，这些数加上 10 个倍数也能表成这种形式，因此在前 1000 个自然数中有 $6\times100=600$ 个数能表成这种形式。

例 3 设 α、β 为正无理数，并且 $\frac{1}{\alpha}+\frac{1}{\beta}=1$， (1)

则数列 $a_n=[n\alpha]$，$b_n=[n\beta]$，$n=1,2\cdots$都是严格递增的，并且

$\{a_n\mid n=1,2\cdots\}\cap\{b_n\mid n=1,2\cdots\}=\varnothing$ (2)

$\{a_n\mid n=1,2\cdots\}\cup\{b_n\mid n=1,2\cdots\}=N$ (3)

证明：由(1)知 $\alpha>1$，$\beta>1$，因此$\{a_n\}$，$\{b_n\}$均为严格递增数列。

任取 $c\in N$，设在$[1,c)$内$\{a_n\}$有 h 项，$\{b_n\}$有 k 项。

则 $[h\alpha]<c\leqslant[(h+1)\alpha]$，即 $h\alpha<c<(h+1)\alpha$

$$h<\frac{c}{\alpha}<h+1，同理有\ k<\frac{c}{\beta}<k+1，$$

故有 $$h+k<\frac{c}{\alpha}+\frac{c}{\beta}<h+k+2$$

$$h+k<c<h+k+2，故\ c=h+k+1，$$

即有 $h+k=c-1$。又由 c 的任意性，在$[1,c+1)$中，$\{a_n\}$，$\{b_n\}$共有 c 项。于是$[c,c+1)$中，$\{a_n\}$和$\{b_n\}$共有一项即 c。

这表明任一自然数 $c\in\{a_n\mid n=1,2\cdots\}\cup\{b_n\mid n=1,2\cdots\}$同时 c 也仅属于两个数列之一。命题得证。

满足(2)和(3)的数列称为互补数列。

例 3 也称为 Beaty 定理，在有关$[x]$的竞赛题中经常出现。

例 4 设 $f,g:Z^+\to Z^+$严格递增函数，

且 $f(Z^+)\cup g(Z^+)=Z^+$，$f(Z^+)\cap g(Z^+)=\varnothing$，

$g(n)=f(f(n))+1$，求 $f(2n)$

解：$\{f(n)\}$，$\{g(n)\}$是互补数列，易知 $f(1)=1$，$g(1)=2$，$f(2)=3$，$f(3)=4$，$g(2)=5$，以此类推，可知

$f(n)$ 1,3,4,6,8,9,11,12…

$g(n)$ 2,5,7,10,13,15,18,20…

受例 3 的启发,先假定 $f(n)=[\alpha n], g(n)=[\beta n]$,其中 α,β 为正无理数,满足$\frac{1}{\alpha}+\frac{1}{\beta}=1$,让我们看看 α,β 应是什么数。

由 $g(n)=f(f(n))+1$,则$[\beta n]=[\alpha[\alpha n]]+1$,两边同除以 n,并令 $n\to+\infty$得 $\beta=\alpha^2$,代入$\frac{1}{\alpha}+\frac{1}{\beta}=1$,得到

$\alpha^2-\alpha-1=0$,则 $\alpha=\frac{1+\sqrt{5}}{2}, \beta=\frac{3+\sqrt{5}}{2}$.

现在证明上面的假定成立,即 $f(n)=[\alpha n], g(n)=[\beta n]$,满足 $g(n)=f(f(n))+1$,即$[\beta n]=[\alpha[\alpha n]]+1$。

事实上 $\alpha[\alpha n]=\alpha(\alpha n-\{\alpha n\})=\alpha^2 n-\alpha\{\alpha n\}<\alpha^2 n-\{\alpha^2 n\}$

即要证 $\alpha\{\alpha n\}>\{\alpha^2 n\}=\{\alpha n+n\}=\{\alpha n\}$

由于 $\alpha\approx1.618>1$,则显然 $\alpha\{\alpha n\}>\{\alpha n\}$

即　$\alpha[\alpha_n]<[\beta_n]$,故$[\alpha[\alpha n]+1]\leqslant[\beta n]$

另一方面$[\beta n]=[(\alpha+1)n]=[\alpha n]+n$

$\alpha[\alpha n]=[\alpha n]\left(1+\frac{1}{\alpha}\right)=[\alpha n]+\frac{1}{\alpha}[\alpha n]>[\alpha n]+\frac{1}{\alpha}(\alpha n-1)=$ $[\alpha n]+n-\frac{1}{\alpha}>[\beta n]-1$

$\alpha[\alpha n]+1>[\beta n]$,即$[\alpha[\alpha n]]+1\geqslant[\beta n]$

综上所述 $g(n)=f(f(n))+1$,则 $f(n)=\left[\frac{1+\sqrt{5}}{2}n\right], g(n)=\left[\frac{3+\sqrt{5}}{2}n\right], f(2n)=[(1+\sqrt{5})n]$

例 5　现有两堆筹码,甲、乙二人按以下规则轮流取:

(a) 如果只动一堆筹码,可以取出任意多根。

(b) 如果动两堆筹码,从两堆中取出的筹码数必须相同。首先把筹码取光的人算赢。问谁有获胜策略?不妨设甲先取,乙后取。

解：设目前两堆筹码数为(m,n)，不妨设$m\leqslant n$当$m=n$时，先取的人必赢。当$m=1$时，设两堆筹码的数目为$(1,n)$，当$n=0,1$时，先取者赢，当$n=2$时，即$(1,2)$，甲取完后，只能变成下列几种形式之一：$(0,2)$，$(1,1)$，$(1,0)$，$(0,1)$，对这四种形式中的哪种情况均是乙赢，规定先取者不能赢的数组叫输数组。故$(1,2)$是输数组，由此知，$(1,n)$当$n>2$时，先取者甲赢，同理对$(2,n)$，先取者甲取走$n-1$根后剩下$(2,1)$，即甲赢。对于$(3,n)$同样的讨论可知$(3,5)$是输数组……仿照以上的方法，可以逐步推出以下的输数组(x_n,y_n)，$n=1,2\cdots$，$(1,2)$，$(3,5)$，$(4,7)$，$(6,10)$，$(8,13)$，$(9,15)$，$(11,18)\cdots$

即 $x_n:1,3,4,6,8,9,11,12\cdots$

$$y_n:2,5,7,10,13,15,18,20\cdots\cdots \tag{4}$$

由例4知 $x_n=\left[\dfrac{1+\sqrt{5}}{2}n\right]$，$y_n=\left[\dfrac{3+\sqrt{5}}{2}n\right]$

如果给定的两堆筹码数(a,b)不是上述的输数组，则总可以经过一次适当的拿取，使之变成输数组，设$a\leqslant b$，易证$\{x_n\}$，$\{y_n\}$是互补数列，则a必在(4)内出现。(ⅰ)若$a=x_n$，$b>y_n$，则可从b中减去$b-y_n$，得到(x_n,y_n)；若$b<y_n$，设$b-a=k<n$则可从a,b内同时减掉x_n-x_k，得到(x_k,y_k)，$k=0$时即得$(0,0)$

(ⅱ)若$a=y_n$，则可从b中减去$b-x_n$，得到(x_n,y_n)或(y_n,x_n)。

由此可知，当甲碰到两堆筹码数构成的不是输数组时，总可以经过一次适当的拿取，使之变成输数组，无论乙怎样取，甲总能保证每次取完后留给乙的是输数组，甲就确保获胜。

当甲碰到的是输数组时，若乙知道这个获胜策略，则甲必输；若乙不知道这个获胜策略，只要有一步失招，甲还可以取胜。

例6 已知一个长方体盒子，可用单位立方体填满。如果改放尽可能多的体积为两个单位的立方体，而且使其与盒子的棱平行，则盒子的容积恰被填满40%，试求出具有此种性质的长方体

形盒子的容积($\sqrt[3]{2}=1.2599\cdots$)。

解:设 Q 为一具有所要求性质的长方体盒子,$a\leqslant b\leqslant c$ 为符合条件的 Q 的边长,由于 Q 内可填满单位立方体,故 a,b,c 均为自然数。现放入体积为 2 的立方体,其棱长为$\sqrt[3]{2}$,故 $a\geqslant 2$ 在长度为 n 的线段上用$\sqrt[3]{2}$的线段去量,只能量$\left[\frac{n}{\sqrt[3]{2}}\right]$次,故这个箱子内共可放入

$\left[\frac{a}{\sqrt[3]{2}}\right]\left[\frac{b}{\sqrt[3]{2}}\right]\left[\frac{c}{\sqrt[3]{2}}\right]$个体积为 2 的立方体,由于其体积为 abc 的 40%,则有

$$2\left[\frac{a}{\sqrt[3]{2}}\right]\left[\frac{b}{\sqrt[3]{2}}\right]\left[\frac{c}{\sqrt[3]{2}}\right]=0.4abc$$

故 $$\frac{a}{\left[\frac{a}{\sqrt[3]{2}}\right]}\cdot\frac{b}{\left[\frac{b}{\sqrt[3]{2}}\right]}\cdot\frac{c}{\left[\frac{c}{\sqrt[3]{2}}\right]}=5$$

为求适合上式的自然数 a,b,c,可先考虑函数

$$g(n)=\frac{n}{\left[\frac{n}{\sqrt[3]{2}}\right]}\quad(n\geqslant 2)$$

列表如下

n	2	3	4	5	6	7	8	9	10	…
$\left[\frac{n}{\sqrt[3]{n}}\right]$	1	2	3	3	4	5	6	7	7	…
$g(n)$	$\frac{2}{1}$	$\frac{3}{2}$	$\frac{4}{3}$	$\frac{5}{3}$	$\frac{6}{4}$	$\frac{7}{5}$	$\frac{8}{6}$	$\frac{9}{7}$	$\frac{10}{7}$	…

当 $n>10$ 时,估计 $g(n)$如下:

$$\frac{\left[\frac{n}{\sqrt[3]{2}}\right]}{n}=\frac{\frac{n}{\sqrt[3]{2}}-\left\{\frac{n}{\sqrt[3]{2}}\right\}}{n}=\frac{1}{\sqrt[3]{2}}-\frac{1}{n}\left\{\frac{n}{\sqrt[3]{2}}\right\}>0.79-\frac{1}{10}=0.69>\frac{2}{3}$$ 故

当 $n>10$ 时，$g(n)<\frac{3}{2}$。

又 $\left[\frac{n}{\sqrt[3]{2}}\right]<\frac{n}{\sqrt[3]{2}}$，故 $g(n)>\frac{n}{\frac{n}{\sqrt[3]{2}}}=\sqrt[3]{2}>1.25$

利用上表可知 $a=2$。因为若 $a>2$，则

$g(a)g(b)g(c)\leqslant\left(\frac{5}{3}\right)^3=\frac{125}{27}<5$，这与 $g(a)g(b)g(c)=5$ 矛盾。

由 $a=2$ 得 $g(b)g(c)=\frac{5}{2}$，于是可推出 $g(b)$ 和 $g(c)$ 中至少有一个大于 $\frac{3}{2}$，因此不外有以下两种情况

(1) $g(b)=2, g(c)=\frac{5}{4}$ 由 $g(n)>1.25$ 知(1)不可能

(2) $g(b)=\frac{5}{3}$ $g(c)=\frac{3}{2}$ 或 $g(c)=\frac{5}{3}, g(b)=\frac{3}{2}$

故 $b=5, c=6$ 或 $b=3, c=5$。

因此箱子 Q 的内部尺寸的所有要能值为(2,5,6)或(2,3,5)。

练 习 一

1. 设$\left[\frac{1}{3-\sqrt{7}}\right]=a$，$\left\{\frac{1}{3-\sqrt{7}}\right\}=b$，

求 $a^2+(1+\sqrt{7})ab+b^2$ 的值。

2. 证明：对任意 $n\in N$，$[(3+\sqrt{5})^n]$是奇数。

3. 求证对任意实数 x,y 都有

$[2x]+[2y]\geqslant[x]+[x+y][y]$

4. 解方程$[x^2]-[x]^2=1993$。

5. 求$[(\sqrt{3}+\sqrt{2})^{1998}]$的个位数字。

6. 设 $t>1$ 是整数，$x\in R$，求证：

$$\sum_{k=0}^{\infty}\left(\left[\frac{x+t^k}{t^{k+1}}\right]+\left[\frac{x+2t^k}{t^{k+1}}\right]+\cdots+\left[\frac{x+(t-1)t^k}{t^{k+1}}\right]\right)$$
$$=\begin{cases}[x] & x\geqslant 0\\ [x]+1 & x<0\end{cases}$$

7. 求证 $2^{n-1}\mid n!\Leftrightarrow n=2^{k-1}$，$k$ 为某一自然数。

8. 位于直线 $y=\frac{1}{2}x-3$，$x=12$ 和 x 轴形成的三角形内部的整点共有多少个？

9. 解方程$[x^2-2x]=[x]^2-2[x]$

10. 求一个正数 x，使得$\{x\}+\frac{1}{\{x\}}=1$ 成立，问 x 能否为有理数？

11. 当$0\leqslant x\leqslant 100$时，求函数 $f(x)=[x]+[2x]+\left[\frac{5}{3}x\right]+[3x]+[4x]$的值集的元素个数。

12. 求 1998! 中末尾 0 的个数。

13. 序列 $n_1,x_2\cdots x_n\cdots$，$x_1=\frac{1}{2}$，$x_{n+1}=x_n^2+x_n$，$n=1,2\cdots$ 若 $S=\frac{1}{x_1+1}+\frac{1}{x_2+1}+\cdots+\frac{1}{x_{100}+1}$，求$[S]$。

14. 计算$[\sqrt{1}]+[\sqrt{2}]+[\sqrt{3}]+\cdots+[\sqrt{n^2-1}]$

15. 在 $m\times n$ 格棋盘的左下角放一棋了,甲,乙二人轮流走棋,每次可以向上,向右,或向右上对角线方向走任意多格,谁先走到右上角谁为胜,问如何获胜?

第四章　不定方程

§1　基本概念

1.1 定义

我们首先考虑一个古老的问题——鸡兔同笼问题：

一只笼子里装有若干只鸡和若干只兔子，已知有 80 条腿，问笼中各有多少只鸡？多少只兔子？

如果令 x 为笼中鸡的数量，y 为兔子的数量则有 $2x+4y=80$，这个方程有无数多组解，如

$$\begin{cases}x=20\\y=10\end{cases}\quad\begin{cases}x=30\\y=10\end{cases}\quad\begin{cases}x=20\\y=30\end{cases}\quad\begin{cases}x=0\\y=20\end{cases}\quad\begin{cases}x=-7.5\\y=23.75\end{cases}$$

但这无数多组解中只有正整数解才能满足题目的要求，求这种方程的整数解和有理数解的问题，是丢番图(Diophalltus)第一个提出并求解的，因此这种方程也称为丢番图方程。

例如 $2x+3y=6, x^2+y^2=z^2, x^2-2y^2=1, x^4+y^4=z^4$

对它们求整数解，但实际上，我国古代提出的勾股定理的一组正整数解 $x=3, y=4, z=5$，比丢番图更早得多。

定义 4.1　不定方程指的是未知数的个数多于方程的个数的整系数方程，且要求它们的解是整数或正整数。

最简单的不定方程就是二元一次不定方程，有时也把特殊形式的未知数的个数多于方程的个数的方程叫不定方程，其解的范围也可相应扩大，如求其有理数解，以下无特殊说明，均求不定方程的题数解。

定义 4.2　方程 $ax+by=c$　叫做二元一次不定方程，其中 a、b、c 为整数。

定理 4.1 不定方程 $ax+by=c$ 有整数解的充要条件是 $(a,b)\mid c$。

证明:必要性,设不定方程 $ax+by=c$ 有解 x_0,y_0,则有 $ax_0+by_0=c$,又$(a,b)\mid a$,$(a,b)\mid b$ 故$(a,b)\mid ax_0+by_0$,即$(a,b)\mid c$

充分性 设$(a,b)=d$,且 $d\mid c$,令 $c=dc_1$

则存在 $x_0,y_0\in Z$,使 $ax_0+by_0=d$,从而有,

$$ac_1x_0+bc_1y_0=c$$

即 $x=c_1x_0,y=c_1y_0$ 就是 $ax+by=c$ 的解

此时有$(a,b)\mid c$,故不定方程 $ax+by=c$ 就是不定方程 $\frac{a}{(a,b)}x+\frac{b}{(a,b)}y=\frac{c}{(a,b)}$,即这两个方程同解。

由于$(a,b)=d$,$d\mid c$,故$\left(\frac{a}{d},\frac{b}{d}\right)=1$,因此以后我们只讨论$(a,b)=1$ 的情形.

1.2 ax+by=c 的特解和通解

由定理 4.1 知,在不定方程 $ax+by=c$ 有解的情况下,总可以假定$(a,b)=1$

定理 4.2 若$(a,b)=1$,且 x_0y_0 为

$$ax+by=c \tag{1}$$

的一组解,则(1)的解都可表为:

$$\begin{cases} x=x_0+bt \\ y=y_0-at \end{cases} \quad t=0,\pm1,\pm2\cdots \tag{2}$$

证明: 由 $ax+by=c$ 和$ax_0+by_0=c$,可得

$$a(x-x_0)+b(y-y_0)=0$$

由于$(a,b)=1$,所以 $a\mid y-y_0$ 令

$$y=y_0-at,$$

则有

$$x=x_0+bt$$

易证由(2)式给出的 x、y 对所有整数 t 都满足不定方程(1)

称 x_0、y_0 为不定方程(1)的一组特解

称由(2)式给出的解为不定方程(1)的通解

若 x_0、y_0 是方程 $ax+by=1,(a,b)=1$ 的特解，则 cx_0,cy_0 是 $ax+by=c$ 的一组解。

求 $3x+5y=7$ 的全部解

解：由于 $(-3)\cdot3+2\cdot5=1$，故 $x_0=-21$ $y_0=14$ 是原方程的一组特解，所以原方程的全部解为

$$\begin{cases} x=-21+5t \\ y=14-3t \end{cases} \qquad t=0,\pm1,\pm2$$

例 1 求不定方程 $50x-35y=85$ 的全部解。

解：原方程等价于 $10x-7y=17$

由于 $(10,7)=1$，故原方程有解

由观察可得一组特解 $x_0=1,y_0=-1$

故原方程的全部解为

$$\begin{cases} x=1-7t \\ y=-1-10t \end{cases} \qquad t=0,\pm1,\pm2\cdots$$

§2 一次不定方程

2.1 方程 $ax+by=c$ 的有关算法

求解不定方程 $ax+by=c$，必须(1)求出最大公约数 $d\nmid(a,b)$，并判断是否有 $d|c$；(2)若 $d\nmid c$，原不定方程无解；(3) 若 $d|c$，则有解。再设法求出一组特解 x_0,y_0，即可得到通解，下面我们通过具体例子来介绍一种判断方程是否有解、及求出其解的直接算法，这种算法对一元一次方程也适用。

例 1 求方程 $24x-439y=158$ 的全部解。

解　$24x=439y+158$

$$x=18y+6+\frac{1}{24}(7y+14)$$

$$m_1=\frac{1}{24}(7y+14) \quad \in Z$$

$$y=\frac{1}{7}(24m_1-14)$$

$$=3m_1-2+\frac{1}{7}(3m_1)$$

$$m_2=\frac{1}{7}(3m_1) \quad \in Z$$

$$m_1=\frac{1}{3}(7m_2)=2m_2+\frac{m_2}{3}$$

$$m_3=\frac{m_2}{3} \quad \in Z$$

$$m_2=3m_3 \quad \in Z$$

$$x=18y+6+m_1$$

$$=18(24m_3-2)+6+7m_3$$

$$=439m_3-30$$

$$y=3m_1-2+m_2$$

$$=21m_3-2+3m_2$$

$$=24m_3-2$$

$$m_1=2m_2+\frac{m_2}{3}$$

$$=2m_2+m_3$$

$$=2\cdot 3m_3+m_3=7m_3$$

∴方程的全部解为 $\begin{cases} x=439m_3-30 \\ y=24m_3-2 \end{cases} \quad m_3=0,\pm 1,\pm 2,\cdots$

其全部正整数解为

$$\begin{cases} x=439m_3-30 \\ y=24m_3-2 \end{cases} \quad m_3=1,2,3\cdots$$

这种解不定方程的算法实际上是对整个不定方程用辗转相除法,依次化为等价的不定方程,直到出现一个变元的系数为 ±1 的不定方程为止(如上例中是 $m_2=3m_3$),这样的不定方程是可以直接解出的,再依次反推上去,就得到了原方程的通解,为了减少运算次数,在用带余除法时,我们总取绝对最小剩余,如果不定方程无解,则在施行这种算法时就会直接看出。

解二元一次不定方程,还可以直接对系数用辗转相除法得到。下面用辗转相除法来求解例 1。

$(24,439)=(24,439-24\times 18)=(24,7)=(24-3\times 7,7)=(3,7)$

$=(3,7-3\times 2)=(3,1)$

即 $1=7-3\times 2=7-(24-3\times 7)\times 2=7\times 7-24\times 2$

$=7\times(439-24\times 18)-24\times 2$

$=439\times 7-(7\times 18+2)\times 24$

$\therefore 1=-(128)\cdot 24+(-7)\cdot(-439)=(-128)\cdot 24-7\cdot(-439)$

$\therefore 158=158(-128)\cdot 24-7\cdot 158\cdot(-439)$

$\therefore x_0=-128\cdot 158,\ y_0=-7\cdot 158$

$x_0=-20224=-46\times 439-30\quad y_0=-1106=-46\times 24-2$

$\therefore$原方程的全部解为

$$\begin{cases}x=-20224-439t\\ y=-1106-24t\end{cases}\qquad t=0,\pm 1,\pm 2,\cdots$$

即$$\begin{cases}x=439t-30\\ y=24t-2\end{cases}\qquad t=0,\pm 1,\pm 2,\cdots$$

2.2 性质定理

下面我们来讨论二元一次不定方程

$$ax+by=c$$

(1) 可解时,它的非负解和正解问题。由(1)的通解公式 $\begin{cases}x=x_0+bt\\ y=y_0-at\end{cases}$ 知道可归结为确定参数 t 的值,使 x,y 的值非负或正。显然当 a,b 异号时,不定方程(1)可解时总有无穷多组非负解或正解,所以只要讨论 a,b 均为正的情形,先来讨论非负解。

定理 4.3 设 a,b,c 均为正整数,$(a,b)=1$,则当 $c>ab-a-b$ 时,不定方程(1)有非负解,其解数等于 $\left[\frac{c}{ab}\right]$ 或 $\left[\frac{c}{ab}\right]+1$;当 $c=ab-a-b$ 时,不定方程(1)无非负解。

证明：由于$(a,b)=1$，故方程(1)必有解，设x_0,y_0是方程(1)的一组特解。则非负解为$x=x_0+bt\geqslant 0$ $y=y_0-at\geqslant 0$，故有$-\frac{x_0}{b}\leqslant t\leqslant\frac{y_0}{a}$，又$t\in Z$，故有$-\left\{\frac{x_0}{b}\right\}\leqslant t\leqslant\left\{\frac{y_0}{a}\right\}$，即$t$可以取下列值：

$$-\left\{\frac{x_0}{b}\right\},-\left\{\frac{x_0}{b}\right\}+1,\cdots,0,1,\cdots\left\{\frac{y_0}{a}\right\}$$

因此方程(1)的非负解的组数为$N_0=\left\{\frac{x_0}{b}\right\}+\left\{\frac{y_0}{a}\right\}+1$又$\left\{\frac{x_0}{b}+\frac{y_0}{a}\right\}\leqslant\left\{\frac{x_0}{b}\right\}+\left\{\frac{y_0}{a}\right\}+1$ 及$\left\{\frac{x_0}{b}\right\}+\left\{\frac{y_0}{a}\right\}\leqslant\left\{\frac{x_0}{b}+\frac{y_0}{a}\right\}$ 故有$\left\{\frac{x_0}{b}+\frac{y_0}{a}\right\}\leqslant N_0\leqslant\left\{\frac{x_0}{b}+\frac{y_0}{a}\right\}+1$

上式的两个等号有且仅有一个成立。由于x_0,y_0是特解，故$ax_0+by_0=C$，所以$\frac{x_0}{b}+\frac{y_0}{a}=\frac{c}{ab}$

故$N_0=\left\{\frac{c}{ab}\right\}$或$N_0=\left\{\frac{c}{ab}\right\}+1$

当$c>ab-a-b$时

$$1-\frac{1}{a}-\frac{1}{b}\leqslant\frac{c}{ab}=\frac{x_0}{b}+\frac{y_0}{a}=\left[\frac{x_0}{b}\right]+\left\{\frac{x_0}{b}\right\}+\left[\frac{y_0}{a}\right]+\left\{\frac{y_0}{a}\right\}$$

$$=\left[\frac{x_0}{b}\right]+\left[\frac{y_0}{a}\right]+\left\{\frac{x_0}{b}\right\}+\left\{\frac{y_0}{a}\right\}$$

$$\leqslant\left[\frac{x_0}{b}\right]+\left[\frac{y_0}{a}\right]+\frac{b-1}{b}+\frac{a-1}{a}$$

即 $1<\left[\frac{x_0}{b}\right]+\left[\frac{y_0}{a}\right]+2$

故有$N_0>0$，即这时必有非负解。

当$c=ab-a-b$时，用反证法证明方程(1)无非负解。若有非负解x_1,y_1，即$ax_1+by_1=ab-a-b$ 则$ab=a(x_1+1)+b(y_1+1)$，由于$(a,b)=1$，则必有$a\mid(y_1+1)$，$b\mid x_1+1$，得$y_1+1\geqslant a$，$x_1+1\geqslant b$

故 $ab=a(x_1+1)+b(y_1+1)\geqslant ab+ba=2ab$,矛盾。

所以当 $c=ab-a-b$ 时,方程(1)无非负解。

定理 4.3 也可表述为:若 $a>0, b>0, (a,b)=1$ 则 $ab-a-b$ 是最大的不能由 $ax+by(x\geqslant0, y\geqslant0)$ 表示出的整数。由此可以推广至三个变数,即 a,b,c 为三个正整数,且 $(a,b,c)=1$,求最大的不可由 $ax+by+cz(x\geqslant0, y\geqslant0, Z\geqslant0)$ 表示出的整数,这个问题已由柯召教授解决。

利用代换 $\mu=x-1, v=y-1$,可推出定理 4.4。

定理 4.4 设 a,b,c 均为正整数,且 $(a,b)=1$,则当 $c>ab$ 时,方程(1)有正解、解数等于

$-\left[-\dfrac{c}{ab}\right]-1$ 或 $-\left[\dfrac{-c}{ab}\right]$,当 $c=ab$ 时,方程(1)无正解。

此定理可以仿照定理 4.3 直接证明,证明略。

例 1 求不定方程 $15x+25y=100$ 的非负解。

解 原方程等价于 $3x+5y=20$

$20>3\times5-3-5$,据定理 4.3 原方程有非负解

易知 $3\cdot40+5(-20)=20$

$\therefore$ $x_0=40, y_0=-20$ 是原方程的一组特解

$\therefore$ 通解为 $\begin{cases}x=40+5t'=5t\\ y=-20-3t'=-3t+4\end{cases}$ $t=0,\pm1,\pm2,\cdots\cdots$

其中非负解是 $0\leqslant t\leqslant\dfrac{4}{3}$

$\therefore$ $t=0$ 或 1,有两组非负解,即

$$\begin{cases}x=0\\ y=4\end{cases}\qquad\begin{cases}x=5\\ y=1\end{cases}$$

例 2 鸡翁一,值钱五,鸡母一,值钱三,鸡雏三值钱一。百钱买百鸡。问鸡翁、母、雏各几何?

解:设 x,y,z 分别代表鸡翁,鸡母和鸡雏的数目,由已知可得

$$\begin{cases}5x+3y+\frac{z}{3}=100\\x+y+z=100\end{cases}$$

消去 Z 后，可得

$$7x+4y=100 \qquad (1)$$

$x_1=0, x_2=25$，是一组特解，(1)的全部非负解是

$$\begin{cases}x=4t\\y=25-7t\end{cases}$$

$0=-\left[\frac{0}{4}\right]\leqslant t\leqslant\left[\frac{25}{7}\right]=3$，即有四组非负解

$$\begin{cases}x=0\\y=25\end{cases}\quad\begin{cases}x=4\\y=18\end{cases}\quad\begin{cases}x=8\\y=11\end{cases}\quad\begin{cases}x=12\\y=4\end{cases}$$

因此所买鸡的各种可能的情形如下表

x	0	4	8	12
y	25	18	11	4
z	75	78	81	84

2.3 多元线性不定方程

定义 4.3 设整数 $k\geqslant 2, c_1, a_1, a_2-a_k$ 是整数且 $a_1, a_2, \cdots a_k$ 都不等于零，以及 $x_1, x_2\cdots x_k$ 仅取整数，方程

$$a_1x_1+a_2x_2+\cdots+a_kx_k=c \qquad (1)$$

称为 k 元一次不定方程，$a_1, a_2, \cdots a_k$，称为它的系数。当 $k>2$ 时，统称为多元一次不定方程。

定理 4.5 不定方程(1)有解的充要条件是$(a_1, a_2\cdots a_k)\mid c$，进而，不定方程(1)有解时，它和$\frac{a_1}{g}x_1+\cdots+\frac{a_k}{g}x_k=\frac{c}{g}$同解，这里 $g=(a_1, a_2\cdots a_k)$。

证明： 必要性　若(1)有解 $x_i=x_{i0}$ $i=1,2\cdots k$，则 $a_1x_{10}+a_2x_{20}+\cdots+a_kx_{k0}=c$

因为$(a_1,a_2,\cdots,a_k)\mid a_i \quad i=1,2,\cdots n$,显然

$(a_1,a_2\cdots a_n)\mid c$

充分性　若 $g=(a_1,a_2,\cdots a_k)$,$g\mid c$,可令 $c=c_1 g$ 存在 l_1,l_2,$\cdots l_k\in Z$,使得 $a_1 l_1+a_2 l_2+\cdots+a_k l_k=g$

从而有 $a_1 l_1 c_1+a_2 l_2 c_2+\cdots+a_k l_k c_1=c_1 g=c$

即方程(1)有解 $x_1=l_1 c_1,x_2=l_2 c_1,\cdots x_k=l_k c_1$

当(1)有解时,必有 $g\mid c$,此时方程(1)与方程$\frac{a_1}{g}x_1+\cdots\cdots+\frac{a_k}{g}x_k=\frac{c}{g}$是同一个方程,故二者同解。

解一般的 k 元一次不定方程可化为解由 $k-1$ 个二元一次不定方程构成的方程组,且它的通解中恰有 $k-1$ 个参数。

定理 4.6　设 $g_1=a_1,g_2=(g_1,a_2)=(a_1,a_2)\cdots$ $g_k=(g_{k-1},a_k)=(a_1,a_2\cdots a_k)$则不定方程(1)等价于下面的 $k-1$ 个方程的不定方程组,它有 $2(k-1)$个整数变数 $x_1,\cdots,x_k,y_2,\cdots,y_{k-1}$

$$\begin{cases} g_{k-1}y_{k-1}+a_k x_k=c \\ g_{k-2}y_{k-1}+a_{k-1}x_{k-1}=g_{k-1}y_{k-1}, \\ \cdots \\ g_2 y_2+a_3 x_3=g_3 y_3 \\ g_1 x_1+a_2 x_2=g_2 y_2 \end{cases} \tag{2}$$

当方程(1)有解时,它的通解由 $k-1$ 个参数的线性表达式给出。

证明:(1) 先证等价性

若 $x_1,\cdots x_k,y_2,\cdots y_{k-1}$是方程组(2)的解,则显然有 $x_1,x_2\cdots x_k$ 是(1)的解。反之若 $x_1,x_2\cdots x_k$ 是(1)的解,则取 $y_j=\frac{1}{g_j}(a_1x_1+\cdots+a_jx_j)$,$2\leqslant j\leqslant k-1$,显然 $y_j\in Z$,且 $x_1,x_2\cdots x_k,y_2,\cdots y_{k-1}$是(2)的解。

(2) 再讨论方程组(2)的解:

方程组(2)的每一个方程有解的充要条件是 $g_k | c$,而其余的方程可以看成是变数为 y_{j-1}, x_j 的二元一次不定方程

$$g_{j-1} \cdot y_{j-1} + a_j x_j = g_j y_j \quad j = k-1, \cdots 2 \tag{3}$$

总是可解的,故一定存在 $y_{j-1}^{(0)}, x_j^{(0)} \in Z$,使得 $g_{j-1} y_{j-1}^{(0)} + a_j x_j^{(0)} = g_j$

这样就有 $y_j y_{j-1}^{(0)}, y_j x_j^{(0)}$ 是(3)的一组特解。

故(3)的通解为 $\begin{cases} y_{j-1} = y_j y_{j-1}^{(0)} + \dfrac{a_j}{g_j} t_{j-1} \\ x_j = y_j x_j^{(0)} - \dfrac{g_{j-1}}{g_j} t_{j-1} \end{cases}$ $t_{j-1} = 0, \pm 1, \pm 2 \cdots$ (4)

$$(2 \leqslant j \leqslant k-1)$$

当(1)有解,即 $g_k | c$ 时,方程组(2)的第一个方程可解,设其特解为 $y_{k-1,0}, x_{k,0}$,则其通解为

$$\begin{cases} y_{k-1} = y_{k-1,0} + \dfrac{a_k}{g_k} t_{k-1} \\ x_k = x_{k,0} - \dfrac{g_{k-1}}{g_k} t_{k-1} \end{cases} \quad t_{k-1} = 0, \pm 1, \pm 2, \cdots \tag{5}$$

将(4)中的 $y_{j-1}, x_j (j = k-1, \cdots 2)$ 依次代入(5),则可得到 $x_1, x_2 \cdots x_k$ 的参数表达式,即为(1)的通解公式。

下面以三元一次不定方程为例来说明如何用定理 4.6 的方法来解 k 元一次不定方程。

例 1 设 $(a, b, c) = 1$,则不定方程

$ax + by + cz = 1$

的全部解是

$$\begin{cases} x = rt + crm + n \dfrac{b}{d} \\ y = st + csm - n \dfrac{a}{d} \\ z = u - dm \end{cases} \tag{6}$$

其中 m, n 是任意整数,r, s 满足 $ar + bs = d = (a, b)$,t, u 满足

$dt+cu=1, r, s, t, u$ 均为整数。

证明：把(6)代入方程 $ax+by+cz=1$。直接验算可知(6)是原方程的解。因此我们只需证不定方程的解具有形式(6)。

设$(a,b)=d$，且存在 $r,s\in Z$，使得 $ar+bs=d$，则 $ax+by=d$ 的通解是$\begin{cases} x=r+\dfrac{b}{d}k \\ y=s-\dfrac{a}{d}k \end{cases}$ $\quad k=0,\pm1,\pm2\cdots$

于是方程 $ax+by=vd, v\in Z$ 的全部解是

$$\begin{cases} x=vr+k\dfrac{b}{d} \\ y=vs-k\dfrac{a}{d} \end{cases} \quad k\in Z, \qquad (7)$$

易知方程 $ax+by+cz=1$ 的整数解，必使 $ax+by$ 为整数，于是只需求 $vd+cz=1$ 的整数解，因为$(d,c)=[(a,b),c]=(a,b,c)=1$

故存在 $t,u\in Z$，使 $dt+cu=1$

所以 $vd+zc=1$ 的通解是$\begin{cases} v=t+mc \\ z=u-md \end{cases}$ $\quad m=1,\pm1,\cdots$

将 v 代入(7)可得

$$\begin{cases} x=rt+crm+k\dfrac{b}{d} \\ y=st+csm-k\dfrac{a}{d} \\ z=u-dm \end{cases}$$

其中 $m,k\in Z, r,s,t,u\in z$，且 $ar+bs=(a,b)-d$，

$(dt+cu)=1$

关于不定方程(1)的非负整数解的问题，有下面的定理

定理 4.7 设 $d_i=(a_1,a_2\cdots a_i), i=2,3,\cdots k, k>1, d_1=a_1$，$d_k=1$，则当 $C>N(a_1,a_2\cdots a_k)=\sum\limits_{i=2}^{k}a_i\dfrac{d_i-1}{d_i}-\sum\limits_{j=1}^{k}a_j$ 时，方程(1)

有整数解 $x_i \geqslant 0, i=1,2,\cdots k$。

证明：对 k 用数学归纳法。

$k=2$ 时，$N(a_1,a_2)=a_1a_2-a_1-a_2$，定理 4.3 知定理成立。

设 $(a_1,a_2\cdots a_{k-1})=d_{k-1}, d_k=1$ 知 $(d_{k-1},a_k)=1$，再设 $a_i=d_{k-1}a'_i, i=1,2,\cdots k-1, d'_i=(a'_1,\cdots a'_i), i=2,\cdots k-1, d'_1=a'_1$，由 $(d_{k-1},a_k)=1$ 可知，对任给的 c，存在 $0\leqq b_k\leqq d_{k-1}-1$，使得 $d_{k-1}\mid c-a_kb_k$，于是由(1)可得

$$a'_1x_1+\cdots+a'_{k-1}x_{k-1}=\frac{c-a_kb_k}{d_{k-1}}=c' \quad (a'_1\cdots a'_{k-1})=1 \quad (8)$$

由于 $c>N(a_1,a_2\cdots a_k)$，故

$$c'=\frac{c-a_kb_k}{d_{k-1}}\geqslant\frac{c-a_k(d_{k-1}-1)}{d_{k-1}}>\sum_{i=2}^{k-1}\frac{a_i}{d_{k-1}}\frac{d_{i-1}}{d_i}-\sum_{j=1}^{k-1}\frac{a_j}{d_{k-1}}$$

$$=\sum_{i=2}^{k-1}a'_i\frac{d_{k-1}d'_{i-1}}{d_{k-1}d_i}-\sum_{j=1}^{k-1}a'_j=N(a'_1\cdots a'_{k-1})$$

由归纳假设(8)有整数解 $x_1\geqslant 0,\cdots,x_{k-1}\geqslant 0$，即当 $c>N(a_1,a_2\cdots a_k)$ 时，(1)有整数解 $x_1\geqslant 0,\cdots,x_{k-1}\geqslant 0, x_k=b_k\geqslant 0$。

定理 4.7 告诉我们，对于 k 元线性型方程 $a_1x_1+\cdots+a_ks_k, a_i>0\ (i=1,2\cdots k), (a_1,\cdots,a_k)=1$，存在一个正整数 $N(a_1,a_2\cdots a_k)$，当 $c>N(a_1,\cdots,a_k)$ 时，n 可表为 $\sum_{i=1}^{k}a_ix_i$ 的形式，其中 $x_j\geqslant 0$，$j=1,2\cdots k$。但是 $N(a_1,\cdots,a_k)$ 却不能表示上述形式，称 $N(a_1,\cdots,a_k)$ 叫做线性型 $a_1x_1+\cdots+a_kx_k$ 的最大不可表数，求 $N(a_1,a_2\cdots a_k)$ 的问题就是著名的弗罗比尼乌斯(Frohenius)问题。

练　习　一

1. 求方程 $179x-287y=4$ 的整数解。

2. 求 $2x+5y=15$ 的正整数解。

3. 某人到银行去兑换一张 d 元和 c 分的支票，出纳员出错，给了他 c 元和 d 分，此人直到用去 23 分后才发觉其错误，此时他发现还有 $2d$ 元和 $2c$ 分，问该支票原为多少钱?

4. 设 $a_1, a_2 \cdots a_n$ 为无限正整数列，且 $a_k < a_{k+1}(k \geqslant 1)$，试证明：存在 a_p, a_q，$(p \neq q)$，使得方程

$a_p x + a_q y = am$　对无限多个 a_m 有正整数解。

5. 设 $a_i, b_i, k_i (i=1,2)$ 是给定的整数，且有 $a_1 b_2 - a_2 b_1 \neq 0$，求存在同时满足

$$a_1 x + b_1 y = k_1 \text{ 与 } a_2 x + b_2 y = k_2$$

的整数 x, y 的充分必要条件。

6. A 说："我们三人共有 100 元"。B 说："对，如果你的钱是现在的 6 倍，我的钱是现在的 $\frac{1}{3}$，我们三人仍有 100 元。"C 说："真不公平，我连 30 元钱都不满。"问每人各有多少钱?

7. 求 $x+2y+3z=41$ 的全部解。

8. (百马问题)100 马、100 瓦，大马驮 3，中马驮 2，两小马驮 1 瓦，最后不剩马和瓦，问大马、中马和小马各有多少?

§3 二次或二次以上的不定方程

3.1 $x^2 + y^2 = z^2$

我国古代数学书《周髀算经》曾提到"勾广三,股修四,弦隅五"指出了不定方程 $x^2 + y^2 = z^2$ 的一个特解。因此求出所有边长为整数的直角三角形,即是求方程

$$x^2 + y^2 = z^2 \tag{1}$$

的所有整数解。

我们称方程(1)的满足 $xyz = 0$ 的解为显然解。$xyz \neq 0$ 的解为非显然解。

若 x_0, y_0, z_0 是(1)的整数解,则显然 $\pm dx_0, \pm dy_0, \pm dz_0$($d \in Z$)也是(1)的解;以及对 x_0, y_0, z_0 的任意的正公约数 g, $\pm \frac{x_0}{g}$, $\pm \frac{y_0}{g}$, $\pm \frac{z_0}{g}$ 也是(1)的非显然解。因此,为了求出全部非显然解,只要求方程(1)满足以下条件的解:

$$x > 0, y > 0, z > 0, (x, y, z) = 1$$

即既约的正解 x, y, z。这样的解称为方程(1)的本原解。

引理 1 不定方程(1)的本原解 x, y, z 必满足条件:

$(x, y) = (y, z) = (z, x) = 1$ 且

x, y 一奇一偶 即 $2 \nmid x + y$

证明: 若 $(x, y) \neq 1$,则有素数 $p \mid x, p \mid y$,由(1)知 $p \mid z^2$,故 $p \mid z$,这与 $(x, y, z) = 1$ 矛盾。

同理可知 $(y, z) = (z, x) = 1$

因为 z, y, z 是两两互素的,所以不能有两个偶数,又不能全是奇数(两奇数的平方和是偶数),所以,必然是两个奇数一个偶数。若 x, y 为奇数,z 为偶数,则有 $4 \mid z^2$,但 $4 \nmid x^2 + y^2$,矛盾。因此 x, y 不能同是奇数。故 x, y 必是一奇一偶。

引理 2　不定方程 $uv=w^2,(u,v)=1$　　(2)

的本原解可以写成公式

$$u=a^2,v=b^2,w=ab \quad a>0,b>0,(a,b)=1 \qquad (3)$$

证明: 1) 设 u,v,w 是(2)的一解。令 $u=a^2u_1,v=b^2v_1,a>0,b>0$,其中 u_1,v_1 不再被任何完全平方数整除,则 $a^2|w^2,b^2|w^2$,因此 $a|w,b|w$,又$(u,v)=1$,故$(a^2,b^2)=1$,进而$(a,b)=1$,故可得 $ab|w$。设 $w=w_1ab$,代入(2)即得

$$u_1v_1=w_1{}^2$$

若 $w_1^2\neq1$,则有一质数 p,满足 $p^2|w_1^2$,但由 u_1,v_1 的定义及$(u_1,v_1)=1$ 可知 $p^2\nmid u_1v_1$,故 $w_1^2=1,u_1v_1=1$,但 u_1,v_1,w_1 都是正数,故 $w_1=u_1=v_1=1$,因此　$u=a^2,v=b^2,w=ab,a>0,b>0,(a,b)=1$

2)(3)式中的 u,v,w 显然满足(2)式。

定理 4.8　不定方程(1)的 x 为偶数的全体本原解由下列公式表出:

$$x=2ab,y=a^2-b^2,z=a^2+b^2$$
$$a>b>0,(a,b)=1,2\nmid(a+b) \qquad (4)$$

证明: (i)(4)是(1)的本原解,因为显然有

$$x^2+y^2=4a^2b^2+(a^2-b^2)^2=(a^2+b^2)^2=z^2$$

$x>0,y>0,z>0,2|x,2\nmid y$,设 $d=(x,y)$,则 $d^2|z^2,d|z$ 因此$d|a^2+b^2,d|a^2-b^2,d|2(a^2,b^2)$　又$(a,b)=1$ 故有 $d=1$ 或 2,又 y 为奇数,故 $d=1$

(ii) 设 x,y,z 是方程(1)的本原解,则 $2|x,(x,y)=1$ 因此 y,z 都是奇数,而

$$\left(\frac{x}{2}\right)^2=\frac{y+z}{2}\cdot\frac{z-y}{2}$$

其中$\left(\frac{z+y}{2},\frac{z-y}{2}\right)=1$,如若不然,设 $d=\left(\frac{z+y}{2},\frac{z-y}{2}\right)\neq1$,则 $d|z,d|y$,因而 $d|x$,故 $d=1$,矛盾。

由引理(2)知 $\frac{z+y}{2}=a^2, \frac{z-y}{2}=b^2, \frac{x}{2}=ab, a>0, b>0, (a,b)=1$

即 $x=2ab, y=a^2-b^2, z=a^2+b^2, a>0, b>0, (a,b)=1$ 由 $y>0$,知 $a>b$,又由 y 是奇数知 a,b 之中一奇一偶。

至此就可以得出(1)的全部解:

(i)显然解:$\begin{cases} x=0 \\ y=\pm a \\ z=\pm a \end{cases}$ $\begin{cases} x=\pm a \\ y=0 \\ z=\pm a \end{cases}$ $a \geqslant 0$

(ii)非显然解

$$x=\pm k(a^2-b^2), y=\pm 2kab, z=\pm k(a^2+b^2)$$

或者 $x=\pm 2kab, y=\pm k(a^2-b^2), z=\pm k(a^2+b^2)$

其中 $a>0, b>0, a>b, (a,b)=1$, k 是任意正整数。

(我们知道一个直角三角形斜边长度的平方等于两直角边的长度的平方和)由勾股定理知,求不定方程(1)的正整数解的几何意义就是求边长为正整数的直角三角形。因此我们也把满足(1)的(x,y,z)叫做勾股数组。

下面从另一角度来看不定方程(1)的几何意义。方程(1)的解 x,y,z,当 $z=0$ 时,必有 $x=y=0$,我们约定只考虑 $z\neq 0$ 的解。

设 $\zeta=\frac{x}{z}, \eta=\frac{y}{z}$ (5)

这样方程(1)就变成了

$$\zeta^2+\eta^2=1 \qquad (6)$$

不定方程(1)的求解问题($z\neq 0$)就等价于求方程(6)的有理数解 ζ,η,在直角坐标平面上,方程(6)表示单位圆周,因此求(6)的有理数解就是求单位圆周上坐标为有理数的点,即有理点。

推论 单位圆周上的整点是:

$$\{\pm 1,0\}, \{0,\pm 1\};$$

不是整点的有理点是:

$$\left\{\pm\frac{a^2-b^2}{a^2+b^2},\pm\frac{2ab}{a^2+b^2}\right\},\left\{\pm\frac{2ab}{a^2+b^2},\pm\frac{a^2-b^2}{a^2+b^2}\right\}$$

$$a>0,b>0,a>b,(a,b)=1$$

例 1 求 $x=40$ 时一切本原的勾股数组

解 $x^2=40^2=1600=4\times400=4\times25\times16=4\times5^2\times4^2$

可令 $u=s^2=5^2,s=5,v=t^2=4^2,t=4$

因此,得 $x=2st=2\times5\times4=40$

$$y=s^2-t^2=5^2-4^2=9$$

$$z=s^2+t^2=5^2+4^2=41$$

验算: $x^2+y^2=40^2+9^2=1681=41^2=z^2$

因为$(40,9,41)=1$,所以勾股数组 40,9,41 是基本的。再由 $x^2=40^2=1600=4\times400=4\times20^2\times1^2$,

可令 $u=s^2=20^2,s=20,v=t^2=1^2,t=1$。

可能得到另一组勾股数,

$$x=2st=2\times20\times1=40$$

$$y=s^2-t^2=20^2-1^2=399$$

$$z=s^2+t^2=20^2+1^2=401$$

验算: $x^2+y^2=40^2+399^2=160801=401^2$

因为 $(40,399,401)=1$,所以 40,399,401 也是基本的。

如果把 x^2 再行分解:

$$x^2=1600=4\times400=4\times400\times1=4\times200\times2$$

$$=4\times100\times4=4\times80\times5=4\times50\times8$$

$$=4\times40\times10=4\times25\times16=4\times20\times20,$$

除去上述两组外,$x^2=4\times100\times4=4\times2^2\times10^2$ 也可能是一组勾股数,经验算为 40,96,104。

$$x^2+y^2=40^2+96^2=10816=104^2=z^2$$

但由于$(40,96,104)=8>1$,所以这组勾股数不是基本的。

此外,在分解式中没有平方数,也就没有可能组成勾股数,更没有基本的勾股数了,所以 $x=40$ 时,只能有两组基本的勾股数:

(40,9,41)和(40,399,401)。

3.2 无穷递降法

1673年,法国数学家费尔马提出了下面的猜测:当 $n>2$ 时,方程

$$x^n+y^n=z^n \tag{1}$$

没有正整数解。这通常称为费尔马大定理(Fermat's Last Theoren),这是因为(Fermat)不加证明地提出了许多数论中的定理,这就是其中的一个,后来大多数结论被证明是对的,个别的被否定了,而唯有这一猜测既没有被证明也没有被否定。直到1994年6月份才由英国著名的数学家 Andrew umles 证明了这个猜测的正确性。这个定理的证明非常复杂,在此略去,下面我们介绍几个有关这一问题的简单情形。

定理 4.9 不定方程 $x^4+y^4=z^2$ (2)

无 $xyz\neq0$ 的解

证明 只证(2)无正整数解即可

若(2)有整数解,则可设 z_0 是使(2)成立的最小正整数。显然,此时必有 $(x,y)=1$,否则 $z=\frac{z_0}{(x,y)}$ 就将是满足(2)且小于 z_0 的正整数了。

由3.1引理1知 x,y 必一奇一偶,不妨设 $2|x$ 于是存在 $u,v\in Z$ 使

$$x^2=2uv,y^2=u^2-v^2,z_0=u^2+v^2$$

$$u>v>0\ (u,v)=1\ u,v\text{ 一奇一偶}$$

若 u 偶 v 奇,则 y^2 被4除的余数是3,这是不可能的,故必为 u 奇 v 偶,记 $v=2a,a\in z$,则

$$\left(\frac{x}{2}\right)^2=ua\quad(u,a)=1$$

于是有 $b,c\in z$,使 $u=b^2,a=c^2,b,c>0,(b,c)=1,2\nmid b$,于是

$$y^2=u^2-v^2=b^4-4c^4$$

故 $$(2c^2)^2+y^2=(b^2)^2 \tag{3}$$
且$(2c^2,y)=1$

对(3)继续利用 3.1 引理 1,又有 $l,m\in z$,使

$$2c^2=2lm,\quad b^2=l^2+m^2,$$
$$l,m>0,\qquad (l,m)=1,$$

这时由 $c^2=lm$ 及$(l,m)=1$ 即知存在 $r,s\in z$,使 $l=r^2,m=s^2$, $r,s>0$ 故

$$b^2=r^4+m^4$$

这样,就有

$$0<b\leqslant b^2=u\leqslant u^2<u^2+v^2=Z_0$$

则 b 是较 z_0 更小的满足(2)的正整数,此与 z_0 的定义矛盾。

我们把 x^{4k},y^{4k},z^{4k} 分别写成$(x^k)^4,(y^k)^4,(z^{2k})^2$,由定理 4.9 就可立即证明 $n=4k$ 时费尔马猜测的正确性。

推论 1 不定方程

$$x^{4k}+y^{4k}=z^{4k}$$

无正整数解,这里 k 是任意正整数。

定理 4.9 中所用的方法称为费尔马无穷递降法,其逻辑步骤是

1^0 若一关于正整数的命题 $P(n)$对若干正整数 n 是正确的,则在此诸 n 中必有一最小者。

2^0 若 $P(n_1)$正确,则必有正整数 $n_2<n_1$,使 $P(n_2)$正确。

如果证明了上述二步,则命题 $P(n)$不能成立。

定理 4.10 不定方程

$$x^2+y^2=z^4 \tag{4}$$

满足条件$(x,y)=1$ 的全部正整数解是

$$x=|6a^2b^2-a^4-b^4|,y=4ab(a^2-b^2),z=a^2+b^2, \tag{5}$$

及 $$x=4ab(a^2-b^2),y=|6a^2b^2-a^4-b^4|,z=a^2+b^2, \tag{6}$$

其中 a,b 为满足以下条件的任意整数:

$$a>0\ b>0,(a,b)=1,2\nmid a+b \tag{7}$$

证明：设 x,y,z 是(4)的正整数解，满足 $(x,y)=1$，因此，x，y,z^2 是方程(1)的本原解，由 3.1 引理 1 知，x,y 为一奇一偶，不妨设 $2\mid y$，由定理 4.8 知，必有

$$x=r^2-s^2, y=2rs, z^2=r^2+s^2 \quad (8)$$

其中 $r>s>0,(r,s)=1,2\nmid r+s$ 因而 r,s,z 也是方程(1)的本原解。若 $2\mid s$，则由定理 4.8 知，

$$r=a^2-b^2, s=2ab, z=a^2+b^2 \quad (9)$$

其中 a,b 满足(注意 $r>s$)

$$a>b>0,(a,b)=1 \quad 2\nmid a+b \quad a^2-b^2>2ab \quad (10)$$

由式(8)，(9)得

$$x=a^4+b^4-6a^2b^2, y=4ab(a^2-b^2), z=a^2+b^2 \quad (11)$$

由式(10)得

$$(\sqrt{2}-1)a>b>0,(a,b)=1,2\nmid a+b \quad (12)$$

若 $2\mid r$ 则可知

$$r=2ab, s=a^2-b^2, z=a^2+b^2 \quad (13)$$

其中 a,b 满足(注意 $r>s$)

$$a>b>0,(a,b)=1,2\nmid a+b,2ab>a^2-b^2 \quad (14)$$

由式(8)，(13)得

$$x=6a^2b^2-a^4-b^4, y=4ab(a^2-b^2), z=a^2+b^2 \quad (15)$$

由式(14)得

$$a>b>(\sqrt{2}-1)a>0,(a,b)=1,2\nmid a+b \quad (16)$$

由式(11)，(15)及式(12)，(16)推出：当 $2\mid y$ 时，解由式(5)，(7)给出，由对称性推出，当 $2\mid x$ 时，解由式(6)，(7)给出，此外，容易直接验证：由式(5)，(6)，(7)给出的 x,y,z 一定是方程(4)满足 $(x,y)=1$ 的解。

例 1 方程 $x^2+y^2+z^2=3xyz$ 称为马尔科夫(MapkoB)方程，使其有整数解的正整数 x，称为马尔科夫数。试证

(1) 若 (x_0,y_0,z_0) 是此方程的一组解，则 $(x_0,y_0,3x_0y_0-z_0)$ 也是此方程的一组解。

(2) 此方程的所有整数解都可由(1),从 $x=y=z=1$ 这个特解得出。

证明:(1) $x_0^2+y_0^2+(3x_0y_0-z_0)^2$

$$=x_0^2+y_0^2+z_0^2+9x_0^2y_0^2-6x_0y_0z_0$$

$$=9x_0y^0-3x_0y_0z_0$$

$$-3x_0y_0(3x_0y_0-z_0)$$

所以$(x_0,y_03x_0y_0-z_0)$也是原方程的一组解。

(2) 设 x,y,z 是原方程的正整数解,现分三种情况进行讨论。首先,若 $x=y=z$,则显然有 $x=y=z=1$。

其次,若 $x-y\neq z$,则有

$$2x^2+z^2=3x^2z$$

于是 $x^2|z^2$,故 $x|z$,故有正整数 w,使 $z=wx$,代入上式即得

$$2+w^2=3wx$$

因而 $w|2$,但 $z\neq x$,故 $w\neq 1$,于是 $w=2$,代入上式后可解得 $x=1$,这时有

$$x=1,y=1,z=2$$

显然 $z=3\cdot1\cdot1-1$,即上式是由 $x=y=z=1$ 代入(1)而得到的。

最后,可设 $x<y<z$,于是由原方程可解得

$$2z=3xy\pm\sqrt{9x^2y^2-4(x^2+y^2)}$$

如果上式右边根号前取减号,则因 $1\leqslant x<y$,就有

$$\sqrt{9x^2y^2-4(x^2+y^2)}$$

$$=\sqrt{x^2+y^2+4x^2(y^2-1)+4y^2(x^2-1)}>xy$$

故 $2z<3xy-xy=2xy$,即 $z<xy$,另一方面,由

$$3xyz=x^2+y^2+z^2<3z^2$$

可得 $xy<z$,上述矛盾表明只能取

$$2z=3xy+\sqrt{9x^2y^2-4(x^2+y^2)},$$

故 $2z>3xy$,由此可知,当 $x<y<z$ 时,必有 $3xy-z<z$。这就表明,若 $x<y<z$ 则由(1)得到的解,将使 $x+y+z$ 减小,因而调

换 x,y,z 的顺序，代入(1)得到的新解将使 $x+y+z$ 的值减小。这样，进行了有限次上述操作后，必将使 x,y,z 中至少有两个相等，从而成为前面已讨论过的两种情况，也即可以从 $x=y=z=1$ 得到。

由 $x=y=z=1$，根据使 $x+y+z$ 增加的顺序，可得下表 $(x\leqslant y\leqslant z)$：

z	1	2	5	13	29	34	89	167	194	233	433	610	985…
y	1	1	2	5	5	13	34	29	13	89	29	233	169…
x	1	1	1	1	2	1	1	2	5	1	5	1	2…

表中第一行是前 13 个马尔科夫数。

此例的证明过程中，对 z 也使用了递降法，但由于有 $x=y=z=1$ 而无法再下降，故费尔马无穷递降法有两种用法：一是用来证明无解，如定理 4.9；一是用来证明有无穷多个解，如此例。

3.3 高次不定方程

在数学竞赛中，有关不定方程的试题很多，解决的方法也很灵活多样，归纳起来常见的有下列几种：

(1) 代数式的恒等变形，特别是代数式的因式分解。

(2) 估计，特别是利用不等式的性质。

(3) 奇偶分析

(4) 换元法

(5) 无穷递降法

(6) 整除性质

(7) 其它

某些不定方程的求解，可能仅利用其中一种方法，但很多题目往往需要几种方法混合使用，特别是对于高次或特殊形式的方程，更要视具体情况具体分析，灵活地解决问题。

例 1 求方程 $x^y=y^x$ 的全部正有理数解。

解：$x=y$ 显然是解，下面不妨设 $y>x$

令 $y=(1+w)x, w\in Q^+$（正有理数集），则

$x^{(1+w)x}=[(1+w)x]^x$

故 $x=(1+w)^{\frac{1}{w}}, y=(1+w)^{1+\frac{1}{w}}$

令 $x=\frac{r}{s}, w=\frac{m}{n}, r, s, m, n\in N$

并且 $(r,s)=(m,n)=1$

故得 $r^m n^n=s^m(m+n)^n$

从而有 $r^m=(m+n)^n, n^n=s^m$

设 P 为 n 的素因子，$p^a \| n$（$p^a | n$ 且 $p^{a+1}\nmid n$）则 $m | an$，从而 $m | a, n=l^m, l\in N$

此时 $s=l^n$，同样 $m+n=k^m, r=k^n, k\in N$ 由 $m+n>n$ 得 $k>l$，即 $k\geqslant l+1$

$m=k^m-l^m\geqslant(l+1)^m-l^m\Rightarrow m=1$

可以除去 $x=y\in Q^+$ 外，其余的解为

$$x=(1+\frac{1}{n})^n, y=(1+\frac{1}{n})^{n+1}, n\in N$$

一般，求不定方程有理数解的问题可以转化为求整数解的问题

例 2 求方程 $2x^n=y^{n-1}$ 的正整数。

解：由于 $2|y$，设 $y=2^l\cdot y_1, 2\nmid y_1$，$x=2^r x_1, 2\nmid x_1$ 于是有 $2^{1+rn}x_1^n=2^{(n-1)l}y_1^{n-1}$ 所以 $1+rn=(n-1)l$。解二元一次不定方程

$$(n-1)l-nr=1 \quad \text{可得}$$

$$l=nt-1, r=(n-1)t-1 \quad (t\geqslant 1)$$

又有 $x_1^n=y_1^{n-1}$，必有 $x_1=u^{n-1}, y_1=v^n$，因而

$x=2^{n-2}(2^{t-1}u)^{n-1}=2^{n-2}m^{n-1}$

$y=2^{n-1}(2^{t-1}v)^n=2^{n-1}k^n$

其中 $n\geqslant 2, m>1, k\geqslant 1$

例 3 求 $x^2+y^2+z^2=3xyz$ (1)

的正整数解。

解　设(x_0, y_0, z_0)是(1)的一组正整数解，不妨设 $x_0 \geqslant y_0 \geqslant z_0$，则易证$(3y_0z_0 - x_0, y_0, z_0)$也是(1)的解。并且 $3y_0z_0 - x_0 = \frac{y_0^2 + z_0^2}{x_0}$是正整数。

现在我们证明在 $y_0 > 1$ 时

$$3y_0z_0 - x_0 < x_0 \tag{2}$$

首先，由(1)得　$3x_0^2 \geqslant 3x_0y_0z_0$

即　$x_0 \geqslant y_0z_0$ (3)

在 $y_0 > 1$ 时

$$2y_0^2z_0^2 = y_0^2z_0^2 + z_0^2y_0^2 > z_0^2 + y_0^2$$

所以　$0 = x_0^2 + y_0^2 + z_0^2 - 3x_0y_0z_0 < x_0^2 - 3x_0y_0z_0 + 2y_0^2z_0^2$

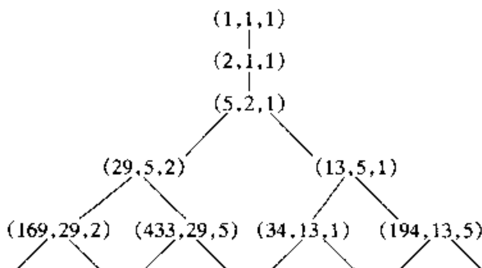
即　$(x_0 - y_0z_0)(x_0 - 2y_0z_0) > 0$

由(3)知　$x_0 > 2y_0z_0$

故(2)式成立

这样从(1)的一组正整数解(x_0, y_0, z_0)，$(x_0 \geqslant y_0 \geqslant z_0)$导出一组新解$(3y_0z_0 - x_0, y_0, z_0)$，并且在 $y_0 > 1$ 时，坐标和 $x_0 + y_0 + z_0$ 严格减少，经过有限步后，必须出现解 $y = z = 1, x = 1$ 或 2。

当 $y = 1$ 时，有解(1,1,1)或(2,1,1)，上面的递降过程至(1,1,1)后，产生的解是(2,1,1)，(2,1,1)产生的解是(1,1,1)，故 $y = 1$ 时递降过程停止，此后不再产生新解，将这一过程递回去，即得到方程(1)的全部解，从(5,2,1)起，每个解(x, y, z)都产生两部解$(3xz - y, x, z)(3xy - z, x, y)$如图



例 4 由费尔马大定理知,当 $n>2$ 时,

$$x^n + y^n = z^n \tag{4}$$

无正整数解。证明方程

$$x^{2n} + y^{2n} = z^2 \tag{5}$$

无正整数解。

证明: 不妨设 $(x,y)=1$,由(5)得

$$x^n = 2uv \quad (u,v)=1, u, v \text{ 一奇一偶} \tag{6}$$

$$y^n = u^2 - v^2 = (u+v)(u-v) \tag{7}$$

在(7)中,$(u+v, u-v) = (u+v, 2u) = (u+v, u) = 1$

所以 $u+v = a^n, u-v = b^n$ (8)

故 $2v = a^n - b^n$ (9)

由(6),在 v 为偶数时

$$2v = c^n \tag{10}$$

由(9),(10)推出,$a^n = b^n + c^n$,与(4)无解矛盾。

在 u 为偶数时,同样可得矛盾。

所以(5)无正整数解。

练　习　二

1. 求方程 $3xy+2y^2-4x-3y-12=0$ 的整数解。

2. 求方程 $x^4+y^4+z^4=2x^2y^2+2y^2z^2+2z^2x^2+24$ 的所有整数解。

3. 求不定方程

$$x^3+x^2y+xy^2+y^3=8(x^2+xy+y^2+1)$$

的所有整数解。

4. 证明两个平方数的和与差不能同为平方数,即方程组

$$y^2+z^2=t^2$$

$$z^2-y^2=x^2$$

无正整数解。

5. 证明方程

$$x^2+y^2-5xy-5=0$$

无整数解。

6. 设 $(lm,n)=1$　则方程

$$x^l+y^m=z^n$$

有无穷多组正整数解。

7. 证明方程

$$5^x=2^y+3^z$$

只有三组整数解,即(1,1,1)(1,2,0)(2,4,2)。

8. 设 a,b,c 为非零整数,已知方程

$$ax^2+by^2+cz^2=0$$

有不同于(0,0,0)的整数解 (x,y,z) 证明方程 $ax^2+by^2+cz^2=1$ 有理数解。

9. 求不定方程 $x^2+y^2+z^2=2xyz$ 的正整数解。

10. 求不定方程 $\sqrt{x}+\sqrt{y}=\sqrt{1989}$ 的整数解。

11. 求不定方程 $\frac{1}{x}+\frac{1}{y}+\frac{1}{z}=\frac{7}{8}$ 的正整数解。

第五章　同　余

§1　同余

1.1　同余的概念

同余是初等数论中的一个基本概念，引入同余简化了数论中许多问题。

定义 5.1　如果用一个正整数 m 去除任意两个整数 a、b，所得的余数相同，即 $a=mq_1+r, b=mq_2+r, 0\leqslant r<m$，我们就说 a、b 对模 m 同余，记作 $a\equiv b(\bmod m)$，如果所得余数不同，我们就说 a、b 对模 m 不同余，记作 $a\not\equiv b(\bmod m)$。模 m 通常为正整数。

如，下列各数哪些对模 7 同余：

$421, 46, 11, -6, -32, 3$

因为 $421=7\times60+1, -6=7\times(-1)+1$，所以

$421\equiv -6\ (\bmod 7)$

同样地 $46=7\times6+4, 11=7\times1+4$

故得 $46\equiv11\ (\bmod 7)$

$-32=7\times(-5)+3 \quad 3=7\times0+3$

故得 $-32\equiv3\ (\bmod 7)$

在日常生活中，也会经常遇到有关同余的问题。如 1998 年的元旦是星期四，问 1999 年元旦是星期几？

1 月 1 日是星期四，1 月 8 日也是星期四，即 $8\equiv1(\bmod 7)$。

由于 $365\equiv1\ (\bmod 7)$，即 1998 年的最后一天是星期四。

所以 1999 年元旦应该是星期五。

1.2 同余的等价命题

由同余的概念,我们容易得到同余的一些等价命题:

定理 5.1 整数 a、b 对模 m 同余的充要条件是 $m \mid a-b$

证明 设 $a=mq_1+r_1, b=mq_2+r_2, 0\leqslant r_i<m(i=1,2)$,若 $a\equiv b(\mathrm{mod}\ m)$,

则 $r_1=r_2$,因此 $a-b=m(q_1-q_2)$,即 $m \mid a-b$,

反之,若 $m \mid a-b$,由 $a-b=m(q_1-q_2)+(r_1-r_2)$,得 $m \mid r_1-r_2$,但 $|r_1-r_2|<m$。故 $r_1-r_2=0$,即 $r_1=r_2$。所以 $a\equiv b(\mathrm{mod}\ m)$。

我们还可以得到同余的另一等价命题:

定理 5.2 a、b 对模 m 同余的充要条件是 $a=mk+b$ 或 $b=mk+a$,其中 $k\in Z$,

证明 设 $a=mq_1+r_1, b=mq_2+r_2, 0\leqslant r_i<m(i=1,2)$,若 $a\equiv b(\mathrm{mod}\ m)$,则 $r_1=r_2$。

$a=mq_1+r_1=mq_1+(b-mq_2)=b+m(q_1-q_2)=b+mk$

同样地,$b=mq_2+r_2=mq_2+(a-mq_1)=a+m(q_2-q_1)=a+mk$。

反之,若 $a=mk+b$,则 $a-b=mk$,

所以 $m \mid a-b$,即有 $a\equiv b(\mathrm{mod}\ m)$

由此我们得到

推论 $a\equiv b(\mathrm{mod}\ m)\Leftrightarrow m \mid a-b\Leftrightarrow a=mk+b$ 或 $b=mk+a$。

灵活应用同余的概念及其等价命题,能大大简化我们的解题过程。

例 1 若 $a\equiv b(\mathrm{mod}\ m)$,则 $(a,m)=(b,m)$。

证明 $\because a\equiv b(\mathrm{mod}\ m)$, $\therefore a=b+mk$ 则 $(a,m)=(b+mk,m)=(b,m)$

例 2 设 p 是素数,试证

$$(a+b)^p\equiv a^p+b^p(\mathrm{mod}\ p)$$

证明 由二项式定理

$(a+b)^p=a^p+c_p^1a^{p-1}b+\cdots+c_p^ia^{p-i}b^i+\cdots+c_p^{n-1}ab^{n-1}+b^p$，又 p 是素数且 c_p^i，$i=1,2,\cdots p-1$ 是整数，故 $p\mid c_p^i$

$$(a+b)^p=a^p+b^p+p(a^{p-1}b+\frac{p-1}{2}a^{n-2}b^2+\cdots+ab^{p-1})$$

所以，$(a+b)^p\equiv a^p+b^p \pmod p$

例 3 （IMO－1－1）证明：对任何自然数 n，分数$\frac{21n+4}{14n+3}$不可约。

证明 设 d 是分子和分母的公约数，于是

$$21n+4\equiv 14n+3\equiv 0 \quad (\bmod d)$$

即

$$21n+4=pd \tag{1}$$

$$14n+3=qd \tag{2}$$

其中 p、q 是正整数。

由(2)×3－(1)×2，得

$$(3q-2p)d=1$$

因为 $3q-2p$ 是整数，所以 $d=1$，故$\frac{21n+4}{14n+3}$不可约。

例 4 （IMO－17－4）设 A 是十进制数 4444^{4444} 的各位数字之和，B 是 A 的各位数字之和，求 B 的各位数字之和。

解 用 $S(n)$ 表示正整数 n 在十进制中各位数字之和。

首先证明

$$S(n)\equiv n \quad (\bmod 9)$$

事实上，设

$$n=a_k10^k+a_{k-1}10^{k-1}+\cdots+a_1\cdot 10+a_0$$

这里 $0\leqslant a_i\leqslant 9$，$a_k\neq 0(0\leqslant i\leqslant k)$，则

$$S(n)=a_k+a_{k-1}+\cdots+a_1+a_0$$

然而

$$n-S(n)=a_k(10^k-1)+a_{k-1}(10^{k-1}-1)+\cdots+a_1(10-1)$$

因为 $10\equiv 1 \pmod 9$，有 $10^i\equiv 1 \pmod 9$，$0\leqslant i\leqslant k$，

所以 $10^i-1\equiv 0 \pmod 9$

故 $n-S(n)\equiv 0 \pmod 9$

即 $s(n)\equiv n \pmod 9$

又因 $4444^{4444}<(4500)^{4444}=(4.5\times 10^3)^{4444}<(10^{\frac{2}{3}+3})^{4444}<10^{16295}$

所以 4444^{4444} 最多是 16295 位数，因此

$$A\leqslant 9\times 16295=146655$$

在不超过 146655 的正整数中，各位数字之和最大的是 99999，因而

$$B\leqslant 45$$

在不超过 45 的正整数，各位数字之和最大的是 39，所以 B 的各位数字之和 $S(B)$ 满足：

$$1\leqslant S(B)\leqslant 12$$

又 $S(B)\equiv B\equiv S(A)\equiv A \pmod 9$，有

$S(4444^{4444})\equiv 4444^{4444}\equiv 7^{4444}\equiv 2^{4444} \pmod 9$

而 $2^{4444}\equiv 2^{3\times 1481+1}\equiv 2\times 8^{1481} \pmod 9$

$\equiv 2\times(-1)^{1481}=-2\equiv 7 \pmod 9$

所以

$$S(B)=7$$

例 5 偶数个人围着一张圆桌坐下讨论问题，休息后，他们重新围着圆桌坐下。证明：至少有两个人休息前后各自所夹的人数相等。

证明： 设有 $2n$ 个人，(i,j) 表示某人休息前后的座位号，若某两人各自休息前后所夹的人数相等，设他们的座位号为 (i_1,j_1)，(i_2,j_2)，则必有 $i_1-j_2\equiv i_2-j_2 \pmod m$

假设任意两个人休息前后各自所夹的人数都不相等，则他们所夹的人数只能是 $0,1,2,\cdots,2n-1$。

所以 $\sum_{k=1}^{2n}(i_k - j_k) = 0 + 1 + \cdots + 2n - 1 = (2n-1)\cdot n$

$$(2n-1)\cdot n \equiv -n \pmod{2n}$$

又 $\sum_{k=1}^{2n}(i_k - j_k) = \sum_{k=1}^{2n} i_k - \sum_{k=1}^{2n} j_k = 0 \equiv 0 \pmod{2n}$

此矛盾说明假设不成立,即至少有两个人休息前后各自所夹人数相等。

练　习　一

1. 今天星期一，再过 1997^{1997} 天后星期几？

2. 求 778^{78} 在 7 进制下的末位数字。

3. 求 13 除 6^{48} 的余数。

4. 求 4 除 $(1^5+2^5+3^5+\cdots+99^5+100^5)$ 所得的余数。

5. 设 N 是正整数，M 是 N 的各个数位上的数字和，求证

$$N \equiv M \pmod 9$$

6. (第 21 届全苏中学生数学竞赛试题)证明，对于任意自然数 n

$$1^{1987}+2^{1987}+\cdots+n^{1987}$$

不能被 $n+2$ 整除。

§2 同余的性质

上一节我们引入了同余的概念讨论了有关等价命题，这一节我们将研究同系的一些基本性质。

定理 5.3 同余是一种等价关系，即满足：

(i) 反身性 $a \equiv a \pmod{m}$

(ii) 对称性 若 $a \equiv b \pmod{m}$，则 $b \equiv a \pmod{m}$

(iii) 传递性 若 $a \equiv b \pmod{m}$，$b \equiv c \pmod{m}$

则 $a \equiv c \pmod{m}$

由同余的定义定理 5.3 是显然的，

定理 5.4 若 $a_i \equiv b_i \pmod{m}$，$i = 1, 2, \cdots, k$，则

(i) $\sum_{i=1}^{k} a_i \equiv \sum_{i=1}^{k} b_i \pmod{m}$

(ii) $\prod_{i=1}^{k} a_i \equiv \prod_{i=1}^{k} b_i \pmod{m}$

证明： (i) $a_i \equiv b_i \pmod{m}$，$i = 1, 2, \cdots, k$

则，$a_i = b_i + mk_i$，$k_i \in Z$，$i = 1, 2, \cdots, k$

$$\sum_{i=1}^{k} a_i = \sum_{i=1}^{k} b_i + m \sum_{i=1}^{k} k_i$$

所以 $\sum_{i=1}^{k} a_i \equiv \sum_{i=1}^{k} b_i \pmod{m}$

(ii) $\prod_{i=1}^{k} a_i = \prod_{i=1}^{k} (b_i + mk_i) = \prod_{i=1}^{k} b_i + mk$，$k \in Z$

所以 $\prod_{i=1}^{k} a_i \equiv \prod_{i=1}^{k} b_i \pmod{m}$

显然，我们可以得出如下推论：

推论 设 k 是整数，n 是正整数，则

(i) 若 $a + b \equiv c \pmod{m}$，则 $a \equiv c - b \pmod{m}$

(ii) 若 $a \equiv b \pmod{m}$，则 $ak \equiv bk \pmod{m}$

(iii) 若 $a \equiv b \pmod{m}$，则 $a^n \equiv b^n \pmod{m}$

由定理 5.4 及其推论容易得到：

定理 5.5 设 $f(x)=\sum_{i=0}^{n}a_ix^i, g(x)=\sum_{i=0}^{n}b_ix^i$ 是两个整系数多项式，满足 $a_i\equiv b_i\ (\mathrm{mod}\ m)\ i=0,1,\cdots,n$，那么若 $a\equiv b\ (\mathrm{mod}\ m)$，则有

$$f(a)\equiv g(b) \quad (\mathrm{mod}\ m)$$

我们称多项式 $f(x),g(x)$ 为 $f(x),g(x)$ 对模 m 同余，记作 $f(x)\equiv g(x)\quad(\mathrm{mod}\ m)$

注意：对所有整数 x，有 $f(x)\equiv g(x)(\mathrm{mod}\ m)$ 成立时，不一定有 $f(x)\equiv g(x)(\mathrm{mod}\ m)$

例如 $x(x-1)(x-2)\cdots(x-m+1)\equiv 0\ (\mathrm{mod}\ m)$，但是显然 $x(x-1)(x-2)\cdots(x-m+1)\not\equiv$ 。$(\mathrm{mod}\ m)$。

对所有整数 x 都成立的同余式 $f(x)\equiv g(x)\ (\mathrm{mod}\ m)$ 称为模 m 的恒等同余式。

定理 5.6 若 $a_1a_2\equiv a_1b_2\quad(\mathrm{mod}\ m)$

$$a_2\equiv b_2 \quad (\mathrm{mod}\ m)$$

且 $(a_2,m)=1$，则 $a_1\equiv b_1\quad(\mathrm{mod}\ m)$

证明 $(a_1-b_1)a_2+b_1(a_2-b_2)=a_1a_2-b_1b_2$，由已知有 $m\mid a_1a_2-b_1b_2$，且 $m\mid a_2-b_2$

所以 $m\mid a_2(a_1-b_1)$ 又 $(a_2,m)=1$

则有 $m\mid a_1-b_1$， 即 $a_1\equiv b_1\quad(\mathrm{mod}\ m)$

此定理特例为：若 $ac\equiv bc\ (\mathrm{mod}\ m)$，且 $(c,m)=1$，则 $a\equiv b\ (\mathrm{mod}\ m)$

定理 5.7 若 $ac\equiv bc\ (\mathrm{mod}\ m)$ 且 $(c,m)=d>1$，则 $a\equiv b\ (\mathrm{mod}\ \frac{m}{d})$

证明 由 $m\mid c\cdot(a-b)$ 得 $\frac{m}{d}\mid\frac{c}{d}(a-b)$

又 $(\frac{c}{d}、\frac{m}{d})=1$，则 $\frac{m}{d}\mid(a-b)$，即 $a\equiv b(\mathrm{mod}\ \frac{m}{d})$

定理 5.8 (i)若 $c>0$，则以下两个同余式同时成立

$$a \equiv b \pmod{m}$$
$$ac \equiv bc \pmod{cm}$$

(ii) 设 $m = \prod_{i=1}^{k} m_i, m_i > 0, i = 1,2,\cdots,k$,
且 $a \equiv b \pmod{m}$,则 $a \equiv b \pmod{m_i}$ $j = 1,2,\cdots,k$

证明 (i) 由 $m \mid a - b \Leftrightarrow cm \mid c(a-b)$,所以(i)成立。

(ii) 由 $m_i \mid m, m \mid a - b$,得 $m_i \mid a - b$ 则命题得证。

定理 5.9 同余式组

$$a \equiv b \pmod{m_j} \quad i = 1,2,\cdots,k$$

同时成立的充要条件是 $a \equiv b \pmod{[m_1, m_2, \cdots, m_k]}$

证明 因为 $m_j \mid a - b$ $(j = 1,2,\cdots,k)$同时成立的充要条件是$[m_1, m_2, \cdots, m_k] \mid a - b$,所以定理成立。

定理 5.10 若 $m \geqslant 1, (a, m) = 1$,则存在 $c \in Z$,使 $ca \equiv 1 \pmod{m}$ $(*)$

我们称 c 是 a 对模 m 的逆,记作 a^{-1}或 $a^{-1} \pmod{m}$

证明 因为$(a, m) = 1$,所以存在 $x_0, y_0 \in Z$,使得 $Ax_0 + my_0 = 1$,取 $c = x_0$ 即得 $ca \equiv 1 \pmod{m}$

显然,$a^{-1} \pmod{m}$不是唯一的,任意整数 c,若 $c \equiv a^{-1} \pmod{m}$,则 c 都是 a 对模 m 的逆;对模 m 的任意两个逆 c_1, c_2,必有 $c_1 \equiv c_2 \pmod{m}$。以后我们提到 a^{-1}或 $a^{-1} \pmod{m}$时是指任意取定的满足$(*)$的 c;对于 a 对模 m 的逆 a^{-1},我们容易得到 $(a^{-1}, m) = 1, (a^{-1})^{-1} \equiv a \pmod{m}$

应用同余的性质,可以使我们的某些运算更方便,以下我们举例说明。

例 1 p 为大于 3 的素数,令

$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} = \frac{a}{b}$,其中 $a, b \in Z$,证明:$p^2 \mid a$。

证明

$$\frac{2}{p} \cdot \frac{a}{b} = \frac{1}{p}\left[\left(1 + \frac{1}{p-1}\right) + \left(\frac{1}{2} + \frac{1}{p-2}\right) + \cdots + \left(\frac{1}{p-1} + 1\right)\right]$$

$$=\frac{1}{p}\sum_{i=1}^{p-1}\frac{p}{i(p-i)}$$
$$=\sum_{i=1}^{p-1}\frac{1}{i(p-i)}$$

对任意 $i\in\{1,2,\cdots,p-1\}$,存在唯一的 $i'\in\{1,2,\cdots,p-1\}$ 满足 $i\cdot i'\equiv 1\pmod p$,且 $i\neq j$ 时,$i'\neq j'$。(证略)

记 $M_i=i'\cdot i\cdot(p-i)\cdot i'$,则 $M_i\equiv -1\pmod p$

这样 $\frac{2a}{pb}=\sum_{i=1}^{p-1}\frac{(i')^2}{M_i}=\frac{k}{m_1m_2\cdots m_{p-1}}$

其中 $k\equiv -\sum_{i=1}^{p-1}(i')^2\equiv -\sum_{i=1}^{p-1}i^2\equiv -\frac{p(p-1)(2p-1)}{b})\pmod p$

$(p,b)=1$,所以 $p\mid k$ (1)

又 $2am_1m_2\cdots m_{p-1}=b\cdot p\cdot k$,$(2m_1m_2\cdots m_{p-1},p)=1$,

所以 $p\mid a$ (2)

由(1)(2)得 $p^2\mid a$。

例 2 设 $n\geqslant 1$,b 的素因子都大于 n,

证明:对任意的正整数 a,必有

$$n!\mid a(a+b)(a+2b)\cdots(a+(n-1)b)。$$

证明 b 的素因子都大于 n,则 $(b,n!)=1$。由定理 5.10 知 b 对模 $n!$ 有逆 b^{-1},则有

$$(b^{-1})^n a(a+b)(a+2b)\cdots(a+(n-1)b)$$
$$\equiv ab^{-1}(ab^{-1}+1)(ab^{-1}+2)\cdots(ab^{-1}+(n-1))\pmod{n!}\quad(1)$$

由于(1)式是 n 个连续整数的积,所以

$$(b^{-1})^n a(a+b)(a+2b)\cdots(a+(n-1)b)\equiv 0\pmod{n!}$$

即有 $a(a+b)(a+2b)\cdots(a+(n-1)b)\equiv 0\pmod{n!}$

命题得证。

例 3 (1901 年匈牙利数学竞赛试题)证明:当且仅当指数 n 不能被 4 整除时,$1^n+2^n+3^n+4^n$ 能被 5 整除,其中 n 是正整数。

证明 $1^4\equiv 1\pmod 5$

$2^4\equiv 1\pmod 5$

$$3^4\equiv 1 \pmod 5$$
$$4^4\equiv 1 \pmod 5$$

即 $a^{4k}\equiv 1 \pmod 5 \quad (a=1,2,3,4)$

设 $n=4k+r$,其中 k 是整数,$r=0,1,2,3$ 由以上易知

$1^n+2^n+3^n+4^n\equiv 1^r+2^r+3^r+4^r \pmod 5$

当 $r=0$ 时,$1^r+2^r+3^r+4^r=4$,故 $5\nmid 1^n+2^n+3^n+4^n$;

当 $r=1$ 时,$1^r+2^r+3^r+4^r=10$,故 $5|1^n+2^n+3^n+4^n$;

当 $r=2$ 时,$1^r+2^r+3^r+4^r=30$,故 $5|1^n+2^n+3^n+4^n$;

当 $r=3$ 时,$1^r+2^r+3^r+4^r=100$,故 $5|1^n+2^n+3^n+4^n$;

综上所述,命题得证。

例 4 (IMO-6-1) (ⅰ)求所有能使 2^n-1 被 7 整除的正整数 n。

(ⅱ)证明:没有正整数 n,使得 2^n+1 被 7 整除。

解 (ⅰ) 因 $2^3\equiv 1 \pmod 7$

由同余性质,有

$$2^{3k}\equiv 1 \pmod 7$$

即 $7|2^{3k}-1$

于是 $2^{3k+1}-1=2(2^{3k}-1)+1$,$2^{3k+2}-1=4(2^{3k}-1)+3$ 都不能被 7 整除。从而,当且仅当 $3|n$ 时,有

$$7|2^n-1$$

证明 (ⅱ)由于 $2^{3k}\equiv 1 \pmod 7$

有 $2^{3k}+1\equiv 2 \pmod 7$

$2^{3k+1}+1\equiv 3 \pmod 7$

$2^{3k+2}+1\equiv 5 \pmod 7$

故对任何 $n\in N$,总有 $7\nmid 2^n+1$。

例 5 设 m 是大于 2 的正奇数,求使 2^{1989} 整除 m^n-1 的最小自然数 n。

解 设 n 为 $2^s q$,其中 q 为奇数,则

$$m^n-1=m^{2^s q}-1=(m^{2^s})^q-1$$

$$=(m^{2^s}-1)((m^{2^s})^{q-1}+(m^{2^s})^{q-2}+\cdots+m^{2^s}+1)$$

$$=(m^{2^s}-1)t$$

其中 $t\equiv1\pmod 2$，于是

$$2^{1989}\mid m^n-1\Leftrightarrow 2^{1989}\mid m^{2^s}-1$$

因此，可设 $n=2^s$，这时有两种情况：

(1) 若 $m\equiv1\pmod 4$，则 m 的二进制表示为 $m=1\cdots\underbrace{100\cdots01}_{k个数字}$，即 k 是使 $m\equiv1\pmod{2^k}$ 的最大整数，于是 $m^2-1=(m+1)(m-1)$ 被 2^{k+1} 整除，而不被 2^{k+2} 整除。设 $m^{2^t}-1$ 被 2^{k+t} 整除而不被 2^{k+t+1} 整除，则

$$m^{2^{t+1}}-1=(m^{2^t}+1)(m^{2^t}-1),$$

被 2^{k+t+1} 整除，而不被 2^{k+t+2} 整除，所以对所有自然数 S。

$$2^{s+k}\mid m^{2^s}-1,2^{s+k+1}\nmid m^{2^s}-1$$

(2) 若 $m\equiv3\pmod 4$，则 m 的二进制表示为 $m=1\cdots0\underbrace{11\cdots1}_{k个数字}$，即 k 为使 $m\equiv-1\pmod{2^k}$ 成立的最大整数。

同样可证对所有自然数 S，

$$2^{s+k}\mid m^{2^s},2^{s+k+1}\nmid m^{2^s}-1,$$

于是，由 $2^{1989}\mid m^{2^s}-1\Rightarrow1989\leqslant s+k$（$k$ 见上面定义）$\Rightarrow s\geqslant 1989-k$。

因而，在 $k\leqslant1989$ 时，最小的指数 $n=2^{1989-k}$，在 $k>1989$ 时，$n=2^0=1$。

练 习 二

1. 设 $m>0$,证明必有一个自然数 a 是 m 的倍数,并且数字全为 0 或 1。

2. 证明从任意的 m 个整数 $a_1,a_2,\cdots,a_m$ 中必可选出若干个数,它们的和(包括只有一个加数的情况)被 m 整除。

3. 设 p 为质数,证明

$$C_n^p \equiv \left[\frac{n}{p}\right] \pmod p$$

这里$[x]$表示 x 的整数部分

4. 设 a,b,c 的十进制表示分别是

$a=\overline{a_n a_{n-1}\cdots a_1 a_0},b=\overline{b_m b_{m-1}\cdots b_0},c=\overline{c_k c_{k-1}\cdots c_0}$

证明 (1) $a\pm b\equiv\sum_{i=0}^{n}a_i+\sum_{i=0}^{m}b_i \pmod 9$

(2) $ab\equiv\sum_{i=o}^{n}a_i\cdot\sum_{i=0}^{m}b_i \pmod 9$

5. 证明(1)两连续整数的立方差不能被 3 整除,(2)若 $a\equiv 1 \pmod{m^k}$,$k>0,m\geqslant 1$,则 $a^m\equiv 1 \pmod{m^{k+1}}$

6. 证明不定方程 $y^2=x^3+23$ 没有整数解。

§3 同余类与代表元

有了同余概念以后，我们可以把数按照同余来分类，于是就自然得出同余类的概念，在某同余类中，我们还需要能代表这类元素特性的代表元。

3.1 基本概念

定义 5.2 以正整数 m 为模，则任何整数必与 $0,1,2,\cdots,m-1$ 之一同余，把同余的数归为一类，不同余的数归为不同的类，则全体整数被分为 m 个类，称为关于模 m 的同余类，我们用 $r \bmod m$ 表示 r 所属的模 m 的同余类。

由同余类的定义立即得到：

定理 5.11 (i) $r \bmod m = \{r + km, k \in Z\}$

(ii) $r \bmod m = s \bmod m$ 的充要条件是 $r \equiv s \pmod m$

(iii) 对任意的 r,s，要么 $r \bmod m = s \bmod m$，要么，$r \bmod m$ 与 $s \bmod m$ 的交集为空集。

定理 5.11 (ii)表明同余式就是同余类(看作一个元素)的等式，因而，关于同余式的性质都可表述为同余类的性质。

关于同余类的个数，我们有：

定理 5.12 对给定的模 m，有且恰有 m 个不同的模 m 的同余类，它们是

$$0 \bmod m, 1 \bmod m, 2 \bmod m, \cdots, (m-1) \bmod m \quad (1)$$

证明 由定理 5.11(ii)知这是 m 个两两不同的同余类，对每个整数 a，由带余除法

$$a = qm + r \qquad 0 \leqslant r < m$$

因此，由定理 5.11(i)知 $a \in r \bmod m$，即 a 必属于(1)中的某个同余类。

为了研究方便，通常把 $0,1,2,\cdots m-1$ 分别称为模 m 的 m 个同余类的代表元。事实上，要研究同余类的问题，只需要研究代表元的问题即可。

由定理 5.12 与抽屉原则立即推出：

定理 5.13 (i) 在任意取定的 $m+1$ 个整数中，必有两个数对模 m 的同余；

(ii) 存在 m 个数两两对模 m 不同余。

证明(i)因为对模 m 共有 m 个由式(1)给出的同余类，所以 $m+1$ 个数中必有两个数属于同一个模 m 的同余类，这两个数就对模 m 同余。

(ii) 在每个同余类 $r \bmod m(0 \leqslant r < m)$ 中取定一个数 x_r 作代表元，这样就得到 m 个两两对模 m 不同余的数 $x_0, x_1, \cdots, x_{m-1}$。

由定理 5.13 可以引进以下概念：

定义 5.3 一组数 $y_1, \cdots, y_s$ 称为是模 m 的完全剩余系，如果对任意的整数 a 有且仅有一个 y_j 是 a 对模 m 的剩余，即 a, y_j 对模 m 同余。在不发生歧义的情况下，也称剩余系或完系。

由定义中 y_j 的唯一性知这 s 个数一定是两两对模 m 不同余，由定理 5.13 知，模 m 的完全剩余系存在，且 $s=m$，以及给定的 m 个数是一组模 m 的完全剩余系的充要条件是它们两两对模 m 不同余。事实上，一组模 m 的完全剩余系就是在模 m 的每个同余类中取定一个数作为代表所构成的一组数；而对于一组模 m 的完全剩余系 $y_1, y_2, \cdots, y_m$。

$$y_1 \bmod m, y_2 \bmod m, \cdots, y_m \bmod m$$

就是模 m 的 m 个两两不同的同余类，以及

$$I = \bigcup_{1 \leqslant j \leqslant m} y_j \bmod m$$

容易验证，下列几组数都是模 m 的完全剩余系：$0, 1, \cdots, m-1$，称为模 m 的最小非负剩余系；$1, 2, \cdots, m$，称为最小正剩余系；$-m+1, -m+2, \cdots, 0$，称为最大非正剩余系；$-m, -m+1, \cdots, -1$，称为最大负剩余系；$-\left[\frac{m}{2}\right]+1, \cdots, 0 \cdots -\left[-\frac{m}{2}\right]$，称为绝对最小剩余系。

易证，任意两组模 m 的完全剩余系，它们各自元素之和对模

m 同余，并且这个和同余于

$$0+1+\cdots+(m-1)=\frac{(m-1)m}{2}\equiv\begin{cases}0 \pmod{m} & 2\nmid m\\ \frac{m}{2} \pmod{m} & 2\mid m\end{cases}$$

下面引进既约同余类，既约剩余系等概念。

定义 5.4 若$(r,m)=1$，则模 m 的同余类 $r \bmod m$ 称为模 m 的既约同余类。

定义 5.5 若$(Z_j,m)=1$，并且对任意整数 a，$(a,m)=1$，有且仅有一个 Z_j，使得 $a\equiv Z_j \pmod{m}$，$1\leqslant j\leqslant t$，则一组数 $Z_1,Z_2,\cdots,Z_t$ 称为是模 m 的既约剩余系，亦称简系。

由定义 5.4 与定理 5.12 立即得到：

定理 5.14 模 m 的所有不同的既约同余类是

$$r \bmod m,(r,m)=1,1\leqslant r\leqslant m$$

例 1 设 n 为偶数，$a_1,\cdots,a_n$ 是模 n 的完系，$b_1,\cdots,b_n$ 也是模 n 的完系，证明

$$a_1+b_1,a_2+b_2,\cdots,a_n+b_n$$

不是模 n 的完系。

证明 因为 $a_1,\cdots,a_n$ 是模 n 的完系，且 $2\mid n$，所以$\sum\limits_{i=1}^{n}a_i\equiv\frac{n}{2}\not\equiv 0 \pmod{n}$

同样地 $\sum\limits_{i=1}^{n}b_i\equiv\frac{n}{2}\not\equiv 0 \pmod{n}$

但是 $\sum\limits_{i=1}^{n}(a_i+b_i)=\sum\limits_{i=1}^{n}a_i+\sum\limits_{i=1}^{n}b_i\equiv\frac{n}{2}+\frac{n}{2}\equiv 0 \pmod{n}$

故 $a_1+b_1,\cdots,a_n+b_n$ 不是模 n 的完系。

例 2 证明从集 $A=\{1,2\cdots,100\}$ 中任取 55 个数，其中必有两个数的差为 10，也必有两个数的差为 12，但不一定含有两个数的差为 11。

解 以 10 为模，将集 A 分为 10 个剩余类，所取的 55 个数中必有 6 个数在同一个剩余类里。

每个剩余类由 10 个数组成，依大小顺序排列时，每两个连续的项相差为 10。上面所说的 6 个数既在同一个剩余类里，必有两个是连续的项(不连续的项至多 5 个)，它们的差当然是 10。

同样，以 12 为模，将集 A 分为 12 个剩余类，所取的 55 个数中若有 6 个数在同一个剩余类里，与上面类似可导出结论(每个剩余类至多含 A 中 9 个数)。

现在设 55 个数中至多有 5 个数在同一个剩余类里。由于

$$55=4\times 12+7$$

因此必有 7 个剩余类里含有 5 个取出的数，但 A 的模 12 的剩余类中，只有 4 个，即

$$\{1,13,25,\cdots,97\},\{2,14,26,\cdots,98\},$$
$$\{3,15,27,\cdots,99\},\{4,16,28,\cdots,100\}$$

是 9 元集，其余的都只含 8 个元素，由于 $7>4$，必有 5 个取出的数在某个 8 元集中，因此其中有 2 个的差为 12。

下面的 55 个数：

1,23,45,67,89,
2,24,46,68,90,
3,25,47,69,91,
4,26,48,70,92,
5,27,49,71,93,
6,28,50,72,94,
7,29,51,73,95,
8,30,52,74,96,
9,31,53,75,97,
10,32,54,76,98,
11,33,55,77,99

中，每两个的差都不等于 11。

例 3 (1956 年北京数学竞赛试题)证明 $n^3+\frac{3}{2}n^2+\frac{1}{2}n-1$

对任何正整数 n 都是整数，并且用 3 除时余 2。

证明 $n^3+\frac{3}{2}n^2+\frac{1}{2}n-1=\frac{n(n+1)(2n+1)}{2}-1$,

由于$\frac{1}{2}n(n+1)$是整数，所以原式对任何整数 n 都是整数。

$$\text{原式}=\frac{2n(2n+1)(2n+2)}{8}-3+2 \qquad (1)$$

由于 $2n(2n+1)(2n+2)$可以被 3 整除，又$(3,8)=1$，因而$\frac{2n(2n+1)(2n+2)}{8}$可以被 3 整除，故(1)式用 3 除余 2。

例 4 （1988 年美国数学竞赛试题）在一个游戏中这样计分，回答一个容易的问题得 3 分，回答一个较难的问题得 7 分，在不能作为选手总分数的整数集合中，求最大值。

解 此题即求集合 $A=\{a \mid a\neq 3n+7m、n,m$ 是非负整数$\}$中数的最大值。

先看 a 可取哪些值，用试验法可知，a 可以取到 0,1,2,4,5,8,11，猜想 11 是集合 A 中的最大数，只需证：凡是不小于 12 的整数 a 都可以表示为 $3n+7m$ 的形式。

a 用 3 除，余数是 0,1 或 2。

若余数为 0，a 当然可表示为 $3n+7m$ 的形式；

若余数为 1，$a=3p+1=3(p-2)+7$；其中 $p\geqslant 2$。

若余数为 2，$a=3p+2=3(p-4)+2\times 7$；其中 $p\geqslant 4$。

故集合 A 中的最大数为 11。

例 5 （IMO－17－2） 设 $a_1,a_2,a_3,\cdots,a_n,\cdots$，是任意一个具有性质 $a_k<a_{k+1}(k\geqslant 1)$的正整数无穷数列，求证：可以把这个数列的无穷多个 a_m 用适当的正整数 x,y 表示为

$$a_m=xa_p+ya_q \quad (p\neq q)$$

证明 依题意，显然 $a_2>1$，而以 a_2 为模的剩余系只有有限个，故必有一个剩余系包含$\{a_n\}$中的无穷多项，设 a_p 是这无穷多项中大于a_2 的最小项。

在上述无穷多项中任取 a_m，必有 $a_m > a_p$，且 $a_m \equiv a_p \pmod{a_2}$，故有自然数 y，使得

$$a_m = a_p + ya_2$$

取 $x = 1, a_q = a_2$，就有

$$a_m = xa_p + ya_q$$

因为 $a_p > a_2$，故知 $p > 2$，所以 $p \neq q$。

这样的 a_m 有无穷多个，故命题成立。

例 6 已知自然数 n 满足 $133^5 + 110^5 + 84^5 + 27^5 = n^5$，试求 n 值。

解 $n^5 \equiv 3^5 + 0 + 4^5 + 7^5 \equiv 3 + 4 + 7 = 4 \pmod{10}$，从而 n 的个位数字是 4。

又 $n^5 < 2 \times 133^5 + (84 + 27)^5 < 3 \times 133^5 < (3125/1024) \times 133^5$

则 $n < 5/4 \times 133 = 167$

故 $n \in \{134, 144, 154, 164\}$

$n^5 \equiv 1^5 + (-1)^5 + 0^5 + 0^5 \equiv 0 \pmod 3$

则 $n \equiv 0 \pmod 3$

因此 $n = 144$。

例 7 F 为 $\{1, 2, \cdots, n\}$ 的一个子集族，满足 (i) 若 $A \in F$，则 $|A| = 3$;

(ii) 若 $A \in F, B \in F, A \neq B$，则 $|A \cap B| \leqslant 1$，设 $f(n) = \max|F|$，证明在 $n \geqslant 3$ 时，

$$f(n) \geqslant \frac{1}{6}(n^2 - 4n)$$

解 考虑 $\{1, 2 \cdots, n\}$ 的三元子集 $\{a, b, c\}$，其中元素满足

$$a + b + c \equiv 0 \pmod n$$

显然 a, b, c 中每一个元素被其它两个完全确定，则满足上式的三元集如果不全相同，则两两至多有 1 个公共元素，即它们所成的集族满足(i)，(ii)。

现在计算$|F|$，由于a有n种选择：$b\neq a$，$n-2a$，$2n-2a$，$\frac{n-a}{2}$，$\frac{2n-a}{2}$（即不使$n(a+b)$或$2n-(a+b)$等于a或b，但b等于$n-2a$与$2n-2a$不会同时发生（前者发生时$a<n/2$，后者发生时$a\geqslant n/2$），所以b至少有$n-4$种选择；c由a，b唯一确定，因此

$$|F|\geq n(n-4)/6$$

即$f(n)\geqslant\frac{1}{6}(n^2-4n)$

3.2 剩余系的结构与性质

为了进一步研究剩余类，本节我们将讨论剩余系的结构与整体性质。

定理 5.15 设a是任意整数，若$x_1,x_2,\cdots,x_m$是模m的完系，则$a+x_1,a+x_2,\cdots,a+x_m$也是模m的完系。

证明 设$k\neq l$，$1\leqslant k<l\leqslant m$，若

$$a+x_k\equiv a+x_l\pmod m$$

则 $x_k\equiv x_l\pmod m$

这与$x_1,x_2,\cdots,x_m$是完系矛盾，即$a+x_1,a+x_2,\cdots a+x_m$这m个数没有两个数对m同余。故是模m的完系。

定理 5.16 若$x_1,x_2,\cdots,x_s$是模m的完系（简系），且$(a,m)=1$，则$ax_1,ax_2,\cdots,ax_s$也是模m的完系（简系）。

证明 当$(a,m)=1$时，对$\forall i,j$，有

$$x_i\not\equiv x_j\pmod m\Leftrightarrow ax_i\not\equiv ax_j\pmod m \tag{1}$$

和

$$(ax_i,m)=(x_i,m) \tag{2}$$

对完系来说，$s=m$，由此及(1)式就得出完系的结论，因为m个数只要两两对模m不同余就一定是模m的完系，但对于简系来说，$s\neq m$（s等于下章所讲的$\phi(m)$）。

定理 5.16 表明：只要$(a,m)=1$，我们总能找到这样的模m的完系和简系，它们的元素都是a的倍数；而当$(a,m)>1$时，这

是一定不可能的。例如 $3\cdot 0,3\cdot 1,\cdots,3\cdot 7$ 是模 8 的完系，取 $a=-1$ 就推出 x 与 $-x$ 同时遍历模 m 的完系。

由以上定理我们也容易得到：

推论　若 $x_1,x_2,\cdots,x_m$ 为模 m 的完系，且 $(a,m)=1$，b 为任意整数，则 $ax_1+b,ax_2+b,\cdots,ax_m+b$ 也是模 m 的完系。

定理 5.17　设 $m_1|m$，那么对任意的 r 有

$$r \bmod m \subseteq r \bmod m_1$$

等号仅当 $m_1=m$ 时成立，确切地说，若 $l_1,\cdots,l_d$ 是模 $d=\frac{m}{m_1}$ 的一组完系，则

$$r \bmod m_1=\bigcup_{1\leqslant j\leqslant d}(r+l_jm_1) \bmod m \tag{3}$$

右边和式中的 n 个模 m 的同余类两两不同。特别地，有 $r \bmod m_1=\bigcup_{0\leqslant j<d}(r+jm_1) \bmod m$　(4)

证明　只证(3)式即可。

我们把同余类 $r \bmod m_1$ 中的数按模 m 来分类，对 $r \bmod m_1$ 中的任意两个数 $r+k_1m_1,r+k_1m_1$

$$r+k_1m_1\equiv r+k_2m_1 \pmod m \Leftrightarrow k_1=k_2$$

则(3)式右边和式中的 d 个模 m 的同余类是两两不同的，且 $r \bmod m_1$ 中的任意一个数 $r+km_1$ 必属于其中一个同余类，另一方面，对任意的 j 必有

$$(r+l_jm_1) \bmod m\subseteq(r+l_jm_1) \bmod m_1=r \bmod m_1$$

命题得证。

若取 $m_1=1,r=0$，则(3)式变为

$$Z=r\ (\bmod 1)=\bigcup_{1\leqslant j\leqslant m}(l_jm_1) \bmod m$$

若 $y_i,i=1,2,\cdots,m$ 是模 m 的完系，则 $Z=\bigcup_{1\leqslant j\leqslant m}y_j \bmod m$。

由此可以得到一个重要的关于剩余系结构的推论：

推论：设 $m=m_1m_2$，$x_i^{(1)}(1\leqslant i\leqslant m_1)$ 模 m_1 的完系，$x_j^{(2)}(1\leqslant j\leqslant m_2)$ 是模 m_2 的完系，那么 $x_{ij}=x_i^{(1)}+m_1x_j^{(2)}$ 是模 m 的完

系，也就是说当 $x^{(1)}, x^{(2)}$ 分别遍历 m_1, m_2 的完系时，$x = x^{(1)} + m_1 x^{(2)}$ 遍历模 $m = m_1 m_2$ 的完系。

这个推论刻画了完系的某种结构：大模 $m_1 m_2$ 的完系，可以用某种形式表示为两较小模 m_1，模 m_2 的完系组合。

定理 5.18 设 $m = m_1 m_2 \cdots m_k$ 及

$$x = x^{(1)} + m_1 x^{(2)} + m_1 m_2 x^{(3)} + \cdots + m_1 m_2 \cdots m_{k-1}{}^{x^{(k)}} \quad (5),$$

那么当 $x^j (1 \leqslant j \leqslant k)$ 是模 m_j 的完系时，x 是模 m 的完系，也就是说 $x_{ij}^{(j)} (1 \leqslant i_j \leqslant m_j)$ 是模 m_j 的完系时 $(1 \leqslant j \leqslant k)$，$x_{i1} x_{i2} \cdots x_{ik} = x_{i1}^{(1)} + m_1 x_{i2}^{(2)} + m_1 m_2 x_{i3}^{(3)} + \cdots + m_1 m_2 \cdots m_{k-1} x_{ik}^{(k)}$ 是模 m 的完系。

证明 $k = 2$ 时，由定理 5.17 推论知结论成立。假设对 $n = k$ 时结论成立，当 $k = n + 1$ 时，$\overline{m}_n = m_1 m_2 \cdots m_n$，以及

$$\overline{x}^{(n)} = x^{(1)} + m_1 x^{(2)} + \cdots + \overline{m}_{n-1} x^{(n)}$$

则有 $\quad x = \overline{x}^{(n)} + \overline{m}_n x^{(n+1)}$

由归纳假设知，当 $x^{(j)} (1 \leqslant j \leqslant n)$ 遍历模 m_j 的完系时，$\overline{x}^{(n)}$ 遍历模 $\overline{m}_n$ 的完系，又 $k = 2$ 时结论成立，可知 $\overline{x}^{(n)}, x^{(n+1)}$ 分别遍历模 $\overline{m}_n$，模 m_{n+1} 的完系时，x 就遍历模 $\overline{m}_n m_{n+1} = m_1 m_2 \cdots m_{n+1}$ 的完系，即结论对 $n = k + 1$ 时成立。

定理 5.19 在定理 5.18 的条件与符号下，设 m_1 与 m 有相同的素因数，那么当 $x^{(1)}$ 遍历模 m_1 的完全（既约）剩余系，$x^{(j)} (2 \leqslant j \leqslant k)$ 分别遍历模 m_j 的完系时，x 遍历模 m 的完全（既约）剩余系。特别地，当 $m_1 = m_2 = \cdots = m_k = n$ 时，当 $x^{(1)}$ 遍历模 n 的完全（既约）剩余系，$x^{(j)} (2 \leqslant j \leqslant k)$ 分别遍历模 n 的完系时，

$$x = x^{(1)} + n x^{(2)} + n^2 x^{(3)} + \cdots + n^{k-1} x^{(k)} \quad (6)$$

遍历模 n^k 的完全（既约）剩余系。

证明 由 m_1 和 m 有相同素因数，则若素数 $p \mid m$，就必有 $p \mid m_1$，又 $m_1 \mid m$，那么

$$(x, m) = 1 \Leftrightarrow (x^{(1)}, m_1) = 1$$

其中 x 由(5)式给出。

由于一个完系中所有与模互素的数构成一个既约剩余系,则由定理 5.18 知命题成立。

定理 5.20 设 $m = m_1 m_2$, $(m_1, m_2) = 1$, $x = m_2 x^{(1)} + m_1 x^{(2)}$ (7)

那么,x 遍历模 m 的完全(既约)剩余系的充要条件是 $x^{(1)}, x^{(2)}$ 同时分别遍历模 m_1, m_2 的完全(既约)剩余系。也就是说,若

$$x_{ij} = m_2 x_i^{(1)} + m_1 x_j^{(2)} \quad (1 \leqslant i \leqslant s, 1 \leqslant j \leqslant t),$$

那么,x_{ij} $(1 \leqslant i \leqslant s, 1 \leqslant j \leqslant t)$ 是模 m 的完全(既约)剩余系的充要条件是:$x_i^{(1)}$ $(1 \leqslant i \leqslant s)$ 是模 m_1 的完全(既约)剩余系,以及 $x_j^{(2)}$ $(1 \leqslant j \leqslant t)$ 是模 m_2 的完全(既约)剩余系。

证 先对完全剩余系来证,先证充分性,这时 $s = m_1, t = m_2$,所以 x_{ij} 共有 $m_1 m_2$ 个数。对任意的 $1 \leqslant i_1, i_2 \leqslant m_1, 1 \leqslant j_1, j_2 \leqslant m_2$,由条件 $(m_1, m_2) = 1$,有

$$x_{i_1 j_1} \equiv x_{i_2 j_2} (\mathrm{mod}\ m)$$

等价于

$$x_{i_1 j_1} \equiv x_{i_2 j_2} (\mathrm{mod}\ m_1), x_{i_1 j_1} \equiv x_{i_2 j_2} (\mathrm{mod}\ m_2),$$

即等价于

$$m_2 x_{i_1}^{(1)} \equiv m_2 x_{i_2}^{(1)} (\mathrm{mod}\ m_1), m_1 x_{j_1}^{(2)} \equiv m_1 x_{j_2}^{(2)} (\mathrm{mod}\ m_2)。$$

这等价于

$$x_{i_1}^{(1)} \equiv x_{i_2}^{(1)} (\mathrm{mod}\ m_1), x_{j_1}^{(2)} \equiv x_{j_2}^{(2)} (\mathrm{mod}\ m_2)。$$

由于 $x_i^{(1)}, x_j^{(2)}$ 分别在同一个模 m_1, m_2 的完全剩余系中取值,所以必有 $i_1 = i_2, j_1 = j_2$。这就证明了这 $m_1 m_2$ 个 x_{ij} 两两对模 m 不同余,即是模 m 的一组完全剩余系。

下证必要性,由 x_{ij} $(1 \leqslant i \leqslant s, 1 \leqslant j \leqslant t)$ 是模 m 的完全剩余系,所以,$st = m = m_1 m_2$。取定 $x_1^{(2)}$,由

$$x_{i1}=m_2x_i^{(1)}+m_1x_1^{(2)},\quad 1\leqslant i\leqslant s$$

对模 $m=m_1m_2$ 两两不同余，所以 $m_2x_i^{(1)}$ 也对模 m_1m_2 两两不同余，即

$$m_2x_{i_1}^{(1)}\not\equiv m_2x_{i_2}^{(1)}(\bmod\ m_1m_2),\quad 1\leqslant i_1\neq t_2\leqslant s。$$

这等价于

$$x_{i_1}^{(1)}\not\equiv x_{i_2}^{(1)}(\bmod\ m_1),$$

即这 s 个 $x_i^{(1)}$ 对模 m_1 两两不同余，所以 $s\leqslant m_1$。同理可证 t 个 $x_j^{(2)}$ 对模 m_2 两两不同余，所以 $t\leqslant m_2$。由此及 $st=m_1m_2$ 推出 $s=m_1$，$t=m_2$，这就证明了必要性。

为了证明对既约剩余系的结论，我们只要证明（为什么）：

$$(x,m_1m_2)=1$$

成立的充要条件是

$$(x^{(1)},m_1)=(x^{(2)},m_2)=1。\tag{8}$$

由于 $(x,m_1m_2)=1$ 等价于

$$(m_2x^{(1)}+m_1x^{(2)},m_1)=(m_2x^{(1)}+m_1x^{(2)},m_2)=1。$$

这就是

$$(m_2x^{(1)},m_1)=(m_1x^{(2)},m_2)=1。$$

由于 $(m_1,m_2)=1$，上式等价于式(8)。

由定理 5.20 利用归纳法，如同证明定理 5.18 一样，立即推出：

定理 5.21 设 $m=m_1\cdots m_k$，$m_1,\cdots,m_k$ 两两既约。再设 $m=m_jM_j(1\leqslant j\leqslant k)$，及

$$x=M_1x^{(1)}+\cdots+M_kx^{(k)}。\tag{9}$$

那么，x 遍历模 m 的完全（既约）剩余系的充要条件是 $x^{(1)},\cdots,x^{(k)}$ 分别遍历模 $m_1,\cdots,m_k$ 的完全（既约）剩余系。

证　$k=2$ 即定理 5.20，所以成立。设 $k=n(\geqslant 2)$ 定理成立，当 $k=n+1$ 时，$m=m_1\cdots m_nm_{n+1}$。设 x 由式(9)$(k=n+1)$给

出，

$$\overline{x}^{(n)}=\frac{m}{m_1m_{n+1}}x^{(1)}+\cdots+\frac{m}{m_nm_{n+1}}x^{(n)}。$$

我们有

$$x=m_{n+1}\overline{x}^{(n)}+\frac{m}{m_{n+1}}x^{(n+1)}。$$

由以上两式，从归纳假设及定理对 $k=2$ 成立，就推出所要结论。

由定理 5.21 及定理 5.16 就推出（证明留给读者）：

定理 5.22 在定理 5.21 的符号和条件下，再设 $a_j(1\leqslant j\leqslant k)$是任意取定的整数，满足$(a_j,m_j)=1\ (1\leqslant j\leqslant k)$。那么，

$$x=a_1M_1x^{(1)}+\cdots+a_kM_kx^{(k)} \tag{10}$$

遍历模 m 的完全（既约）剩余系的充要条件是 $x^{(j)}(1\leqslant j\leqslant k)$分别遍历模 m_j 的完全（既约）剩余系。

例 1 利用模 3 的剩余系来表示 $3^n(n\geqslant 2)$的剩余系。

解 由定理 5.19 知，当 $x^{(1)}$遍历模 3 的完全（既约）剩余系，$x^{(j)}(2\leqslant j\leqslant n)$遍历模 3 的完全剩余系时，

$$x=x^{(1)}+3x^{(2)}+\cdots+3^{n-1}x^{(n)}$$

遍历模 3^n 的完全（既约）剩余系，特别地，$x^{(1)}=0,1,2$（或 1，2），$x^{(j)}=0,1,2(2\leqslant j\leqslant n)$时，$x$ 遍历模 3^n 的最小非负完全（或既约）剩余系；取 $x^{(1)}=1,2,3$（或 1，2），$x^{(j)}=0,1,2(2\leqslant j\leqslant n)$时，$x$ 遍历模 3^n 的最小正完全（或既约）剩余系；取 $x^{(1)}=-1,0,1$（或 -1、1），$x^{(j)}=-1,0,1(2\leqslant j\leqslant n)$时，$x$ 遍历模 3^n 的绝对最小完全（或既约）剩余系。

利用绝对完全最小剩余系的表示法，我们可以得出一个有趣的应用。

例 2 天平的两个托盘上都可以放置砝码，证明可用重量分别为 1 克，3 克，3^2 克，…，3^{n-1}克的 n 个砝码在天平上称出重量在 1 克到$\frac{3^n-1}{2}$克之间的物体的重量。（误差不超过 1 克）

证明 由于砝码有三种放法:放左、放右、不放,可用 $-1,1,0$ 表示这三种放法,而 $-1,0,1$ 恰好是模 3 的绝对最小完系。由定理 5.19 可知:当 $x^{(1)}$遍历模 3 的完系,$x^{(j)}(2\leqslant j\leqslant n)$遍历模 3 的完系时,$x=x^{(1)}+3x^{(2)}+\cdots+3^{n-1}x^{n}$遍历模 3^n 的完系,取 $x^{(j)}=-1,0,1\ (1\leqslant j\leqslant n)$时,$x$ 遍历模 3^n 的绝对最小完系,即 $-\frac{3^n-1}{2},\cdots,-1,0,1,2,\cdots,\frac{3^n-1}{2}$,所以可用 1 克,3 克,$\cdots$,$3^{n-1}$克的砝码称出重量是 1 克,2 克,$\cdots$,$\frac{3^{n-1}}{2}$克的物体。

例 3 设 $m>0,(a,m)=1$,b 是整数,证明:若 x 遍历模 m 的完系,则

$$\sum_{x}\left\{\frac{ax+b}{m}\right\}=\frac{1}{2}(m-1)$$

证明 当 x 遍历模 m 的完系时,由定理 5.16 推论知 $ax+b$ 遍历模 m 的完系,则

$$\begin{aligned}\sum_{x}\left\{\frac{ax+b}{m}\right\}&=\frac{0}{m}+\frac{1}{m}+\cdots+\frac{m-1}{m}\\&=\frac{1}{m}(0+1+2+\cdots+m-1)\\&=\frac{1}{2}(m-1)\end{aligned}$$

例 4 设 n 为偶数,$a_1,a_2,\cdots,a_n$ 是模 n 的完全剩余系,$b_1,b_2,\cdots,b_n$ 也是模 n 的完全剩余系,证明

$$a_1+b_1,a_2+b_2,\cdots,a_n+b_n$$

不是模 n 的完全剩余系。

证明 由于 n 为偶数,即有

$$2\nmid n+1$$

然而

$$n\nmid\frac{n(n+1)}{2}$$

对于模 n 的任意一个完全剩余系，$a_1, a_2, \cdots, a_n$。

$$a_1 + a_2 + \cdots + a_n \equiv 1 + 2 + \cdots + n - \frac{n(n+1)}{2} \not\equiv 0 \pmod{n}$$

同样地

$$b_1 + b_2 + \cdots + b_n \equiv \frac{n(n+1)}{2} \not\equiv 0 \pmod{n}$$

但是

$$(a_1 + b_1) + (a_2 + b_2) + \cdots + (a_n + b_n) \equiv n(n+1) \equiv 0 \pmod{n},$$

所以

$$a_1 + b_1, a_2 + b_2, \cdots, a_n + b_n$$

不是模 n 的完全剩余系。

例 5 设 $m \in N$，$(a, m) = 1$，当 x 遍历模 m 的简系时，

$$\sum_x \left\{ \frac{ax}{m} \right\} = \frac{s}{2}$$

其中 s 是不超过 m 且与 m 互素的数的个数。

证明 设 $x_1, x_2, \cdots, x_s$ 是模 m 的简系，$(a, m) = 1$，则由定理 5.16 知 $ax_1, \cdots, ax_s$ 也是模 m 的简系。

$$\sum_x \left\{ \frac{ax}{m} \right\} = \sum_x \left\{ \frac{mq_i + r_i}{m} \right\} = \sum_{i=1}^{s} \left\{ \frac{r_i}{m} \right\}$$

这里 $r_1, r_2, \cdots, r_s$ 是模 m 的最小正简系，又在模 m 的最小正简系中，r_i 与 $m - r_i$ 是成对出现的(因为 $(r_i, m) = 1$，所以 $(m - r_i, m) = 1$)。

则 $$2\sum_{i=1}^{s} \left\{ \frac{r_i}{m} \right\} = \sum_{i=1}^{s} \left\{ \frac{r_i}{m} \right\} + \sum_{i=1}^{s} \left\{ \frac{m - r_i}{m} \right\} = \sum_{i=1}^{s} 1 = S$$

故 $$\sum_x \left\{ \frac{ax}{m} \right\} = S/2$$

例 6 能否将整数集合分成三个子集 Z_1, Z_2, Z_3，满足 $Z_1 \cup Z_2 \cup Z_3 = Z$，$Zi \cap Zj = \phi (1 \leqslant i \neq j \leqslant 3)$，使得 $n, n - 50, n + 1998$ 分别属于不同集合？

解 假设 Z_1, Z_2, Z_3 满足题设，且 $n, n - 50, n + 1998$ 分别属

于不同集合 Z_1, Z_2, Z_3。引进符号:(1) $m \sim k$ 表示 m, k 属于某一子集。

(2) (m, n, l) 表示 m, n, l 取自三个不同子集。

由 $(n, n-50, n+1998)$ 每一数同减去 50,或同加上 1998 仍然属于三个不同子集。

即 $(n-50, n-100, n+1948)$ 且 $(n+1998, n+1948, n+2\cdot1998)$ 由此可见

$$n+1948 \not\sim n-50$$

$$n+1948 \not\sim n+1998$$

又由 $(n, n-50, n+1998)$ 知 $n \not\sim n-50, n \not\sim n+1998$

故 $n \sim n+1948$

所以有 $(n-50, n-100, n)$,从而 $(n-100, n-150, n-50)$

则 $n \sim n-150$

这样,由 $n \sim n+1948, n-150$ 可推出

$0 \sim 1948 \sim 2\cdot1948 \sim \cdots \sim 50\cdot1948 = 650 \times 150 - 100 \sim 649 \times 150 - 100 \sim \cdots \sim 100$

即 $n \sim n-100$,与 $n \not\sim n-100$ 矛盾。

故 不能将 Z 分成这样的三个子集。

练　习　三

1. 设 $f(x,y)=x^2+kxy+y^2$,问是否存在整数 k,使得当 x,y 取遍所有整数时,$f(x,y)$的值能布满整数集 Z?

2. 设 p 是奇素数,a 是连续数列 $2,3,4,\cdots,p-3,p-2$ (1) 中的任一数,则数列 $a,2a,3a,\cdots,(p-3)a,(p-2)a,(p-1)a$ (2) 中必有一个且只有一个数关于模 p 与 1 同余,设此数为 ia,则 i 为(1)中的数且与 a 相异。

3. 设 p 为奇素数,则

$$2\cdot3\cdots(p-2)\equiv1 \pmod p$$

4. 设$(a,m)=1$,证明方程

$$ax\equiv b \pmod m$$

在$\{0,1,2,\cdots,m-1\}$中有唯一解。

5. 是否可从 10^6 个 6 位电话号码中选出 10^5 个,在同时删去第 k 位,($k\in\{1,2,3,4,5,6\}$后,得到的都是从 00000 到 99999 的全体 5 位号码?

6. 30 对夫妻围着圆桌坐下,证明至少有两名妻子到各自丈夫的距离相等。

7. 设 $a,b,x_0\in N$

$$x_n=ax_{n-1}+b \quad n=1,2,\cdots$$

证明　$x_1,x_2,\cdots$,不可能都是负数。

8. 等差数列由 $n>2$ 个正负数组成,公差 $d>0$,证明 $\prod\limits_{p<n}p\mid d$,其中 p 为小于 n 的负数。

9. 设 $a_1,a_2,\cdots,a_n$ 为无限正整数,且 $a_k<a_{k+1}(k\geqslant1)$,证明:存在 $a_p,a_q(p\neq q)$使得方程对无限多个 a_m 有正整数解。

10. $k_i(1\leqslant i\leqslant s)$是任意整数,那么 $y_1,y_2,\cdots,y_s$ 是模 m 的一组简系的充要条件是 $y_1+k_1m,y_2+k_2m,\cdots,y_s+k_sm$ 是模 m 的一组简系。

第六章　欧拉定理与威尔逊定理

§1　欧拉函数

1.1　基本概念

定义 6.1　对任意正整数 m，数列

$$0,1,2,\cdots m-1 \tag{1}$$

中与 m 互素的数的个数，称为欧拉函数，记为 $\varphi(m)$。

由第五章可知，模 m 的既约剩余系是

$$r \bmod m,(r,m)=1,1\leqslant r\leqslant m$$

所以模 m 的一个既约系内元素的个数就是 $\varphi(m)$。

当 $m=1$ 时，模 1 的同余类只有 0mod1，故 $\varphi(1)=1$；模 2 的同余类有两个，0 mod2 和 1mod2，只有 1mod2 是既约剩余类，故 $\varphi(2)=1$；同理易知 $\varphi(3)=2,\varphi(4)=2,\varphi(5)=4$，等等。当 p 为素数时，$\varphi(p)=p-1$。

定理 6.1　（ⅰ）存在 $\varphi(m)$ 个数，两两对模 m 不同余且均与 m 互素。

（ⅱ）在任意取定的 $\varphi(m)+1$ 个均与 m 互素的整数中，必有两数对模 m 同余。

例如 $m=4$ 时，$\varphi(4)=2$ 模 4 的一组既约剩余系是 1mod 4，3 mod4，故存在 $\varphi(m)=2$ 个数，对模 4 不同余且均与 4 互素。

证明略。

1.2　欧拉函数的计算

已经知道当 p 为素数时，$\varphi(p)=p-1$，下面研究当 $m=p^k$（p 为素数）时，其欧拉函数的表达式。

引理 1　设 p 是素数，$k\geqslant1$，那么

$$\varphi(p^k)=p^{k-1}(p-1) \qquad (2)$$

且模 p^k 的既约剩余系是

$$(a+bp)\bmod p^k \quad 1\leqslant a\leqslant p-1 \quad 0\leqslant b\leqslant p^{k-1}-1 \qquad (3)$$

证明:$\varphi(p^k)$等于满足以下条件的 r 的个数

$$1\leqslant r\leqslant p^k, 且(r,p^k)=1$$

由于 p 是素数,故$(r,p)=\begin{cases}1 & p\nmid r\\ p & p\mid r\end{cases}$,而$(r,p^k)=1$ 的充要条件是$(r,p)=1$,即 $p\nmid r$,因此 $\varphi(p^k)$就等于 $1,2,\cdots,p^k$ 中不能被 p 整除的数的个数,而 $1,2,\cdots,p^k$ 中能被 p 整除的数有 p^{k-1}个,故 $\varphi(p^k)=p^k-p^{k-1}=p^{k-1}(p-1)$。

由带余除法知,任一 r,$1\leqslant r\leqslant p^k$,$p\nmid r$ 可表示为

$r=bp+a \quad 1\leqslant a\leqslant p-1,0\leqslant b\leqslant p^{k-1}$;反之任一满足 $1\leqslant a\leqslant p-1,0\leqslant b\leqslant p^{k-1}-1$ 的 a,b 相应的 $r=bp+a$ 必满足 $p\nmid r$,且 $1\leqslant r\leqslant p^k$,引理得证。

例如 $m-8$ 时,$\varphi(2^3)=2^3-2^2=4$,模 8 的一组既约剩余系是 $(a+2b)\bmod 8 \quad 1\leqslant a\leqslant 1,0\leqslant b\leqslant 2^2-1$,即 $1\bmod 8,3\bmod 8,5\bmod 8,7\bmod 8$ 是模 8 的既约剩余系。

引理 2 $(m,n)=1$,则 $\varphi(mn)=\varphi(m)\varphi(n)$

证明:设 $x_1,x_2\cdots x_{\varphi(m)}$是模 m 的既约剩余系,$y_1,y_2\cdots y_{\varphi(n)}$是模 n 的既约剩余系,则 $y_{i_j}=nx_i+my_j$ 是模 mn 的既约剩余系。这时 r_{ij} $1\leqslant i\leqslant\varphi(m),1\leqslant j\leqslant\varphi(n)$,共有 $\varphi(m)\cdot\varphi(n)$个,下证它们两两对模 mn 不同余,若 $r_{i_1 j_1}\equiv r_{i_2 j_2}(\bmod\ mn)$

$$即\ nx_{i_1}+my_{j_1}=nx_{i_2}+my_{j_2}(\bmod\ mn)$$

$$则\ nx_{i_1}\equiv nx_{i_2} \quad (\bmod\ m)$$

$$由于(n,m)=1,则\ x_{i1}\equiv x_{i2} \quad (\bmod m)$$

由于 x_{i1},x_{i2}在同一模 m 的既约剩余系中取值,故有 $x_{i1}=x_{i2}$,以及必有 $my_{j1}\equiv my_{j2}(\bmod\ mn)$,故有 $y_{j1}\equiv y_{j2}(\bmod n)$,同理可知

$y_{j1} \equiv y_{j2}$。

最后证$(nx_i+my_j, mn)=1$。设$(nx_i+my_j, mn)=d$,则$d \mid nx_i+my_j$,$d \mid mn$,由于$(n,m)=1$,不妨设$d \mid n$,$d \nmid m$,则由$d \mid my_j$,有$d \mid y_j$,即$d \mid (y_j, n)$　故$d=1$,$(r_{ij}, mn)=1$,故有$\varphi(mn)=\varphi(m)\cdot\varphi(n)$。

由引理2可得,若$m_1, m_2 \cdots m_r$两两互素,则

$\varphi(m_1 \cdot m_2 \cdots m_r)=\varphi(m_1)\varphi(m_2)\cdots\varphi(m_r)$

由上述两个引理,就可得到下述定理。

定理6.2　设m的标准分解式为$p_1^{\alpha_1} p_2^{\alpha_2} p_r^{\alpha_r}$,其中$p_1, p_2 \cdots p_n$为互不相同的素数,$\alpha_i \geqslant 1 (i=1,2\cdots r)$,则

$$\varphi(m)=\prod_{k=1}^{r} p_k^{\alpha_k-1}(p_k-1)=\prod_{k=1}^{r}(p_k^{\alpha_k}-p_k^{\alpha_k-1})。$$

推论　若$n \mid m$,则$\varphi(n) \mid \varphi(m)$

例1　n为自然数,$\varphi(n)$或者等于1,或者是偶数。即当$n>2$时,$\varphi(n)$恒为偶数。

证明:$\varphi(1)=\varphi(2)=1$。下证$n>2$时,$\varphi(n)$为偶数。
首先,当$n=2^k$,$k \geqslant 2$,则$\varphi(n)=2^{k-1}$是偶数。

当$n=p^k m$(p为奇数,$k \geqslant 1$),则$\varphi(n)=\varphi(p^k)\varphi(m)=p^{k-1}(p-1)\varphi(m)$由于$p-1$为偶数,故$\varphi(n)$为偶数。

例2　自然数N仅含有质因数3,5,7,且$\varphi(N)=3600$。求N。

解:令$N=3^{\alpha_1}5^{\alpha_2}7^{\alpha_3}$,则$\varphi(N)=3^{\alpha_1-1}5^{\alpha_2-1}7^{\alpha_3-1}(3-1)(5-1)(7-1)=3600$

$$2^4 \cdot 3^{\alpha_1} \cdot 5^{\alpha_2-1} 7^{\alpha_3-1}=2^4 \cdot 3^2 \cdot 5^2 \cdot 7^0$$

故$\alpha_1=2, \alpha_2=3, \alpha_3=1$

$$N=3^2 5^3 7=7875$$

例3　若n是大于1的自然数,它有r个不同的素因数,则$\varphi(n) \geqslant n\dfrac{1}{2r}$;若$n$有$r$个不同的奇素因数,则$2^r \mid \varphi(n)$。

证明:设 $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$,$p_i$ 为互不相同的素数,$\alpha_i\geqslant 1$,$i=1,2,\cdots,r$,则 $\varphi(n)=\prod_{i=1}^{r}p_i^{\alpha_i-1}(p_i-1)=\prod_{i=1}^{r}p_i^{\alpha_i}(1-\frac{1}{p_i})=n\prod_{i=1}^{n}(1-\frac{1}{p_i})$ $\geqslant n\prod_{i=1}^{r}(1-\frac{1}{2})=n\cdot\frac{1}{2r}$。若所有的 p_i 均为奇数,则

$$\varphi(n)=n\prod_{i=1}^{r}(1-\frac{1}{p_i})=\frac{n}{p_1p_2\cdots p_r}\prod_{i=1}^{r}(p_i-1)$$

p_i-1 是偶数($i=1,2,\cdots,r$),$\frac{n}{p_1p_2\cdots p_r}$是整数,故 $2^r\mid\varphi(n)$

例 4 设 m 是自然数,$(a,m)=1$。证明

(ⅰ)当 x 通过模 m 的完全剩余系时,$\sum_x\left\{\frac{ax+b}{m}\right\}=\frac{m-1}{2}$

(ⅱ)当 x 通过模 m 的既约剩余系是,$\sum_x\left\{\frac{ax}{m}\right\}=\frac{\varphi(m)}{2}$

其中$\{x\}$表示 x 的分数部分。

证明:首先说明:若$(m,x)=1$,则$(m-x,m)=1$。并且 $1\leqslant x\leqslant m$ 时 $m>m-x\geqslant 1$。事实上,若$(m,m-x)=d$,则 $d\mid m$,$d\mid m-x$,

故 $d\mid x$,$d\mid(m,x)$,即 $d=1$ 下面只证明(ⅱ)。

如果 $x_1,x_2\cdots x_{\varphi(m)}$是模 m 的简系,$(a,m)=1$,则

$ax_1,ax_2\cdots ax_{\varphi(m)}$ 也是模 m 的简系,从而 $\sum_x\left\{\frac{ax}{m}\right\}=\sum_x\left\{\frac{x}{m}\right\}$不妨设$x_i<m$,$i=1,2\cdots\varphi(m)$。这时$\sum_x\left\{\frac{x}{m}\right\}=\sum_x\frac{x}{m}$

故 $2\sum_x\frac{x}{m}=\sum_x\frac{x}{m}+\sum_x\frac{m-x}{m}=\sum_x 1=\varphi(m)$

即$\sum_x\left\{\frac{ax}{m}\right\}=\frac{\varphi(m)}{2}$。

1.3 欧拉函数的基本性质

引理 2 指出,两个互素数之积的欧拉函数等于这两个数的欧拉函数之积,下面继续讨论两个正整数积的欧拉函数。

定理 6.3 (ⅰ)设 $m=m_1m_2$,若 m_1 与 m_2 有相同的素因数,则

$$\varphi(m)=m_2\varphi(m_1)=m_1\varphi(m_2)$$

（ⅱ）设$(m,n)=d$，则 $\varphi(mn)=\varphi(m)\varphi(n)\frac{d}{\varphi(d)}$

证明：（ⅰ）设 $m_1=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}\quad \alpha_i\geqslant 1,i=1,2,\cdots,r$

$$m_2=p_1^{\beta_1}p_2^{\beta_2}\cdots p_r^{\beta_r}\quad \beta_i\geqslant 1,i=1,2,\cdots,r。$$

则 $m=m_1m_2=\prod_{i=1}^{r}p_i^{\alpha_i+\beta_i}$，又 $\varphi(m)=m\prod_{i=1}^{r}(1-\frac{1}{p_i})$，$\varphi(m_1)=m_1\prod_{i=1}^{r}(1-\frac{1}{p_i})$

故 $\varphi(m)=m_2\varphi(m_1)=m_1\varphi(m_2)$

（ⅱ）$\varphi(mn)=mn\prod_{p|mn}(1-\frac{1}{p})=mn\dfrac{\prod_{p|m}(1-\frac{1}{p})\prod_{p|n}(1-\frac{1}{p})}{\prod_{p|(m,n)}(1-\frac{1}{p})}$

$$=\frac{m\prod_{p|m}(1-\frac{1}{p})\cdot n\prod_{p|n}(1-\frac{1}{p})}{\prod_{p|d}(1-\frac{1}{p})}$$

故 $\varphi(mn)=\dfrac{\varphi(m)\varphi(n)}{\frac{\varphi(d)}{d}}=\varphi(m)\varphi(n)\dfrac{d}{\varphi(d)}$

欧拉函数是一种典型的积性函数，即满足

定义 6.2 若函数 $f(n)$满足下列条件：

（ⅰ）$f(n)$对任意正整数有定义，且至少存在一个正整数 a，使 $f(a)\neq 0$。

（ⅱ）若$(m,n)=1$，则 $f(mn)=f(m)f(n)$。

则称 $f(n)$为积性（可乘）函数。若条件（ⅱ）不要求 m 与 n 互素，即对任意的正整数 m,n 均有$f(mn)=f(m)f(n)$，则称 $f(n)$为完全积性函数。

如 $\varphi(24)=\varphi(4\times 6)=8\neq\varphi(4)\varphi(6)$

$8=\varphi(24)=\varphi(3\times 8)=\varphi(3)\varphi(8)$

由定理 6.3 知，欧拉函数不是完全积性函数。由积性函数的

定义可知，只要讨论了积性函数 $f(n)$ 在所有素数幂上值的结构，$f(n)$ 在正整数集上值的形式就清楚了，从前面对欧拉函数的讨论可看出，欧拉函数的表达式正是沿着这样的思路逐步得出的，这也体现了积性函数的重要性。

积性函数有下面基本性质

定理 6.4 (i) 如果 $f(n)$ 是一个积性函数，则 $f(1)=1$

(ii) 若 $f(n)$ 和 $g(n)$ 都是积性函数，则 $h(n)=f(n)\cdot g(n)$ 也是积性函数。

证明：(i) 由定义知一定存在一个正整数 a，使 $f(a)\neq 0$，由于 $(a,1)=1$，$f(a)=f(a\times 1)=f(a)f(1)$，从而 $f(1)=1$。

(ii) 当 $n=1$ 时，$h(1)=f(1)g(1)=1$ 故 $h(n)$ 不恒为零。若 a,b 是两个正整数，而且 $(a,b)=1$，则

$$h(ab)=f(ab)g(ab)=f(a)f(b)g(a)g(b)=h(a)h(b)$$

即 $h(n)$ 是积性函数。

最后，我们给出欧拉函数的另一个重要性质，先证一个引理：

引理 3 若 $n=\alpha\beta$，则不大于 n 而与 n 以 α 为最大公约数的数的个数为 $\varphi(\beta)$

证明：不大于 n 而与 n 以 α 为公约数的数是：$\alpha,2\alpha,\cdots\beta\alpha$。若 $(k\alpha,n)=\alpha$，即 $(k\alpha,\alpha\beta)=\alpha$ 即 $(k,\beta)=1,1\leqslant k\leqslant\beta$，而这样的 k 共有 $\varphi(\beta)$ 个，故引理 3 得证。

为了叙述方便，引入下述符号。

$s(\alpha)=\{m\mid(m,n)=\alpha,1\leqslant m\leqslant n\}$，由引理 3 知 $|s(\alpha)|=\varphi\left(\frac{n}{\alpha}\right)$。很容易得到下面两条性质：

(1) $s(\alpha_i)\cap s(\alpha_j)=\varphi \quad (\alpha_i\neq\alpha_j)$

事实上，没有一个介于 1 与 n 之间的数，与 n 的最大公约数既是 α_i 又是 α_j。

(2) $\bigcup\limits_{\alpha\mid n}s(\alpha)=\{1,2,\cdots n\}$

对任意的 $1 \leqslant m \leqslant n$，均有 $\alpha \mid n$，使 $(m, n) = \alpha$，取 $\alpha = (m, n)$ 即可。

由以上两条性质可知 $\sum\limits_{d \mid n} \varphi(d) = \sum\limits_{d \mid n} |s(d)| = n$。故有下述定理。

定理 6.5 （高斯公式），自然数 n 的所有正因数的欧拉函数值之和等于 n。即当 $n \geqslant 1$ 时，有 $\sum\limits_{d \mid n} \varphi(d) = n$。

采用将 $1,2,\cdots n$ 分成互不相交的 T 类的方法证明高斯公式。

证明：设 $1 = d_1 < d_2 < \cdots < d_T = n$ 为 n 的全体约数。其中不大于 n 而与 n 以 d_1 为最大公约数的数有 $\varphi(d_T)$ 个，由于 $n = d_1 d_T = d_2 d_{T-1} = \cdots = d_T d_1$ 不大于 n 而与 n 以 d_2 为最大公约数的数有 $\varphi(d_{T-1})$ 个，$\cdots$ 不大于 n 而与 n 以 d_T 为最大公约数的数有 $\varphi(d_1)$ 个，故 $n = \varphi(d_1) + \cdots + \varphi(d_T)$。即 $n = \sum\limits_{d \mid n} \varphi(d)$。

例如 20 有 6 个因数 1,2,4,5,10,20，必有

$20 = \varphi(1) + \varphi(2) + \varphi(4) + \varphi(5) + \varphi(10) + \varphi(20) = 1 + 1 + 2 + 4 + 4 + 8$。

例 1 设 $n > 1$，则 $\sigma(n) = \frac{1}{2} n\varphi(n)$，其中 $\sigma(n)$ 表示不大于 n 而与 n 互素的数之和。

证明：若 $(n, \alpha) = 1$，则 $(n, n - \alpha) = 1$，设 $\alpha_1, \alpha_2 \cdots \alpha_{\varphi(n)}$ 为不大于 n 而与 n 互素的数的全体，则 $n - \alpha_1, n - \alpha_2 \cdots n - \alpha_{\varphi(n)}$ 也是不大于 n 且与 n 互素的数的全体，由 $\sigma(n) = \sum\limits_{i=1}^{\varphi(n)} \alpha_i = \sum\limits_{i=1}^{\varphi(n)} (n - \alpha_i)$

故 $2\sigma(n) = \sum\limits_{i=1}^{\varphi(n)} n = n \cdot \varphi(n)$　即证明了 $\sigma(n) = \frac{1}{2} n\varphi(n)$。

例如 $\sigma(420) = \frac{1}{2} \times 420 \times \varphi(2^2 \times 3 \times 5 \times 7) = 210 \times 2 \times 2 \times 4 \times 6 = 20160$。

例 2 求满足下面等式的所有正整数 m 和 n。

$$\varphi(mn) = \varphi(m) + \varphi(n)$$

解：设 $d = (m, n)$　则 $\varphi(mn) = \varphi(m)\varphi(n)d / \varphi(d) = \varphi(m) + \varphi(n)$

$$\frac{1}{\varphi(m)}+\frac{1}{\varphi(n)}=\frac{d}{\varphi(d)}, \text{即} \frac{\varphi(d)}{\varphi(m)}+\frac{\varphi(d)}{\varphi(n)}=d \qquad (4)$$

由于 $d=(m,n)$ 故 $\varphi(d)\mid\varphi(m)$, $\varphi(d)\mid\varphi(n)$, $\frac{\varphi(d)}{\varphi(m)}\leqslant 1$, $\frac{\varphi(d)}{\varphi(n)}\leqslant 1$

记 $a=\frac{\varphi(m)}{\varphi(d)}$, $b=\frac{\varphi(n)}{\varphi(d)}$, 当 $d>2$ 时,(4)式无解,故 $d=1$ 或 2。当 $d=1$ 时,由 $\frac{1}{a}+\frac{1}{d}=1$ 知 $a=2=b$, $\varphi(m)=\varphi(n)=2$, 经验证只有 $m=4, n=3$ 或 $m=3, n=4$。

当 $d=2$ 时, $a=b=1$, $\varphi(m)=\varphi(n)=1$, 只有 $m=n=2$。

综上所述,满足方程 $\varphi(mn)=\varphi(m)+\varphi(n)$ 的解为

$$\begin{cases} m=4 \\ n=3 \end{cases} \quad \begin{cases} m=3 \\ n=4 \end{cases} \quad \begin{cases} m=2 \\ n=2 \end{cases}$$

练　习　一

1. 试证使 $\varphi(m)=14$ 的自然数 m 不存在。

2. 证明

(1)若 n 是奇数,则 $\varphi(2n)=\varphi(n)$

(2)若 n 是偶数,则 $\varphi(2n)=2\varphi(n)$

3. 证明

(1)$\varphi(4k+2)=\varphi(2k+1)$

(2)$\varphi(4k)=2\varphi(2k)$

4. 证明 $\varphi(n)\geqslant\frac{n}{d(n)}$,其中 $\varphi(n)$,$d(n)$分别为 n 的欧拉函数值和约数个数。

5. 利用 $\varphi(m)$的公式证明有无限多个素数。

6. 证明:若 $6|n$,则 $\varphi(n)<\frac{1}{3}n$。

7. 若 N 为仅具有 200…0 或 500…0 形式的数,且不大于 N 与 N 互质的数的个数是 80,求 N。

8. 设 $n=p_1^{k_1}\cdots p_r^{k_r}$,若用 $\varphi(n,l)$表示从 1 到 l 这 l 个自然数中与 n 互素的数的个数,那么

$$\varphi(n,l)=l-\sum_{i=1}^{r}\left[\frac{l}{p_i}\right]+\sum_{1\leqslant i<j=r}\left[\frac{l}{p_ip_j}\right]+\cdots+(-1)^r\left[\frac{l}{p_1p_2\cdots p_r}\right]$$

§2 欧拉定理与威尔逊定理

2.1 费尔马(Fermat)定理

定理 6.6 (费尔马定理)若 p 为素数,则 $a^p \equiv a \pmod{p}$ (5)

费尔马定理对解决数学竞赛题有着广泛的应用,我们先给出一个初等证明。

证明:不妨假设 a 为非负整数,对 a 作数学归纳。

当 $a=0$ 或 1 时,(5)式成立

当 $p|a$ 时, (5)式成立

假设 a 为大于 1 的任意整数,当 $a=n$ 时,命题成立,则当 $a=n+1$ 时

$(n+1)^p-(n+1)=n^p-n+(c_p^1n^{p-1}+c_p^2n^{p-2}+\cdots+c_p{}^{p-1}n=n^p-n+p\cdot N$

由归纳法知 $p|n^p-n$,故 $p|(n+1)^p-(n+1)$,即$(n+1)^p\equiv n+1 \pmod{p}$从而(5)式对于任意非负整数 a 均成立。定理得证。

推论:若 p 为素数,$(a,p)=1$,则 $a^{p-1}\equiv 1 \pmod{p}$

此推论常称为费尔马小定理。

例 1 求证 $199|\sum_{i=1}^{200} i^{198}$

证明:199 是素数,故$(i,199)=1$,$i=1,2\cdots200$

故 $i^{198}\equiv 1 \pmod{199}$ $i=1,2\cdots198$

又 $199^{198}\equiv 0 \pmod{199}$,$200\equiv 1 \pmod{199}$

故$\sum_{i=1}^{200} i^{198}\equiv \underbrace{1+1+\cdots+1}_{共198个}+0+1=199\equiv 0 \pmod{199}$ 即 $199|\sum_{i=1}^{200} i^{198}$

例 2 求证当 n 为奇数时,$4^n(2^{2n+1}-1)$的十进位数的末两位数是 28。

证明:设 $n=2k+1$,需证 $2^{4k+2}(2^{4k+3}-1)\equiv 28 \pmod{100}$

只需证　$2^{8k+3}-2^{4k}-7\equiv 0\ (\mathrm{mod}\ 25)$

由于$(2,5)=1$,故 $2^4\equiv 1(\mathrm{mod}\ 5)$,$2^{4k}\equiv 1\ \mathrm{mod}\ 5$

$2^{8k+3}-2^{4k}-7=8\cdot 2^{8k}-2^{4k}-7=(2^{4k}-1)(2^{4k+3}+7)$

由于 $2^{4k+3}+7\equiv 2^3+7\equiv 15\equiv 0(\mathrm{mod}\ 5)$,　故 $5|2^{4k+3}+7$

因此有 n 为奇数时,$4^n(2^{2n+1}-1)\equiv 28(\mathrm{mod}\ 25)$。

故当 n 为奇数时,$4^n(2^{2n+1}-1)$的十进位数的末两位数是 28。

例 3　假设 p 是质数,a,b 是任意二个整数,求证

$(a+b)^p\equiv a^p+b^p\quad(\mathrm{mod}\ p)$

证明:若 $p|a$ 且 $p|b$,结论显然成立,若 a,b 二者之一能被 p 整除,不妨令 $p|b$,则

$(a+b)^p\equiv a^p+bq_1\equiv a^p+b^p(\mathrm{mod}\ p)$结论成立。

现设 $p\nmid a$,且 $p\nmid b$,据费尔马定理有　$a^p\equiv a(\mathrm{mod}\ p)$　$b^p\equiv b$ $(\mathrm{mod}\ p)$

即有 $a^p+b^p\equiv a+b(\mathrm{mod}\ p)$,由费尔马定理知$(a+b)^p\equiv(a+b)$ $(\mathrm{mod}\ p)$

得$(a+b)^p\equiv(a+b)\equiv a^p+b^p$

例 4　试证对任意自然数 a,$A=2003a^{12}+2007$ 不是完全平方数

证明:若 $13|a$,则 $A\equiv 2007\equiv 5(\equiv\mathrm{mod}\ 13)$

若 $13\nmid a$,则 $A\equiv 2003+2007\equiv 6\equiv(\mathrm{mod}\ 13)$

下证对任意的完全平方数 m^2 被 13 除不能余 5 或 6。

令 $m=13k+r$　$(10\leqslant r<13)$　当 $r=0$ 时,m^2 除以 13 余数为 0。假设 $m^2=13^2k^2+13\times 2kr+r^2\equiv 5$ 或 6　(mod 13)

即有 $r^2\equiv 5$　(mod 13)　或 $r^2\equiv 6$ (mod 13)　$1\leqslant r\leqslant 12$ 经验证 1,2…12 中任一数的平方模 13 均不为 5 或 6,

故 $2003a^{12}+2007$ 不是完全平方数。

例 5　求证 $f(x)=\frac{1}{5}x^5+\frac{1}{2}x^4+\frac{1}{3}x^3-\frac{1}{30}x$ 为整值多项式

所谓整值多项式是指:一个多项式 $f(x)=a_nx^n+a_{n-1}x^{n-1}$

$+\cdots+a_1x+a_0(ai\in R, i=0,1\cdots n)$，当 x 取任意整数时，$f(x)$ 的值均为整数。显然，当 $a_i\in z$ 时，$f(x)$ 一定为整值多项式，但当 a_i 不全为整数时，$f(x)$ 也可能为整值多项式。如 $f(x)=\frac{1}{3}x(x^2-1)$ 是整值多项式。

证明：由费尔马定理知　$p\mid n^p-n$　（p 为质数）

故 $g(x)=\sum_{p_i}\frac{x^{p_i}-x}{p_i}$ 是整值多项式。

$f(x)=\frac{1}{5}(x^5-x)+\frac{1}{2}(x^4-x)+\frac{1}{3}(x^3-x)-\frac{1}{30}x+\frac{1}{5}x+\frac{1}{2}x+\frac{1}{3}x$

$f(x)=\frac{1}{5}(x^5-x)+\frac{1}{3}(x^3-x)+\frac{1}{2}x(x-1)(x^2+x+1)+x$

由于 $2\mid x(x-1)$，又 $\frac{1}{5}(x^5-x)+\frac{1}{2}x(x-1)(x^2+x+1)+x$ 是整值多项式

故 $f(x)$ 是整值多项式。

关于整值多项式，有如下的定理

定理 6.7　多项式 $f(x)$ 是整值多项式的充要条件是存在整数 $a_1,a_2\cdots a_n$，使 $p(x)=a_n\binom{x}{n}+a_{n-1}\binom{x}{n-1}+\cdots+a_1\binom{x}{1}+a_0\binom{x}{0}$　　(6)

其中 $\binom{x}{0}=1,\binom{x}{k}=\frac{x(x-1)-(x-k+1)}{k!}$　　$(k\in N)$

证明：充分性，只须证 $\binom{x}{k}$ 是整数即可。

当 $m\geqslant k$ 时，$\binom{m}{k}=\frac{m(m-1)-(m-k+1)}{k!}=c_m^k$

当 $0\leqslant m\leqslant k-1$ 时，$\binom{m}{k}=0$

当 $m<0$ 时，令 $m=-m_0, m_0>0$，

则 $\binom{m}{k}\frac{-m_0(-m_0-1)\cdots(-m_0-k+1)}{k!}=$

$(-1)^k\frac{(m_0+k-1)\cdots(m_0+1)m_0}{k!}$

$\binom{m}{k}=(-1)^k C_{m_0+k-1}^k=(-1)^k C_{-m+R-1}^k$是整数。

由于 $a_i(i=0,1,\cdots n)$是整数，故 $f(x)$是整值多项式。

必要性

设 $p(x)$是 n 次整值多项式，对 n 归纳。

当 $n=0$ 时显然

设 $p(x)$是 $n+1$ 次整值多项式

任一个 k 次多项式 $Q(x)$都可以唯一地表示成

$$Q(x)=\alpha_k\binom{x}{k}+\alpha_{k-1}\binom{x}{k-1}+\cdots+\alpha_1\binom{n}{1}+\alpha_0,(\alpha_i\in R)\ (7)$$

因为只要令 $x=0,1,\cdots k$，通过(7)式就可以逐个确定出 $\alpha_1,\alpha_2\cdots\alpha_k$ 的值，并且(7)式是唯一的。

设 $p(x)=a_{n+1}\binom{x}{n+1}+a_n\binom{x}{n}+\cdots+a_1\binom{x}{1}+a_0, a_i\in R$，

下证系数 $a_1,a_2\cdots a_{n+1}$ 都是整数

显然 $p(x+1)$也是整值多项式。故 $f(x)=p(x+1)-p(x)$是整值多项式，由于当 $r\geqslant 1$ 时有

$$\binom{x+1}{r}-\binom{x}{r}=\frac{(x+1)x\cdots(x-r+2)}{r!}-\frac{x(x-1)\cdots\cdots(x-r+1)}{r!}$$

$$=\frac{x(x-1)\cdots(x-r+2)}{r!}(x+1-x+r-1)$$

$$=\binom{x}{r-1}$$

故 $f(x)=a_{n+1}\binom{x}{n}+a_k\binom{x}{n-1}+\cdots+a_2\binom{x}{1}+a_1\binom{x}{0}$

$f(x)$是 n 次整值多项式，由归纳假设知 $a_1,a_2\cdots a_{n+1}$都是整数，又 $p(0)=a_0$ 也是整数，故 $a_0,a_1,\cdots a_{n+1}$都是整数。

用此定理来判断 $p(x)$是否为整值多项式，计算往往比较繁锁，下面给出另一个判定定理。

定理 6.8 k 次多项式 $p(x)$为整值多项式的充要条件是 x 取某$k+1$ 个连续整数时，$p(x)$的值都是整数。

证明:必要性显然。

对 k 用归纳法证明充分性。

$k=0$ 时显然。假设结论对 k 次多项式成立。

设 $p(x)$是 $k+1$ 次多项式，当 $x=n,n+1,\cdots,n+k+1$ 时，$p(x)$取整数，令 $p(x)=a_{k+1}\binom{x}{k+1}+a_k\binom{x}{k}+\cdots+a_1\binom{x}{1}+a_0$，$(a_i\in R)$。

$Q=p(x+1)-p(x)=a_{k+1}\binom{x}{k}+a_k\binom{x}{k-1}+\cdots+a_2\binom{x}{1}+a_1\binom{x}{0}$在 $k+1$ 个连续整数 $n,n+1\cdots n+k$ 上取整数值。故 $Q(x)$是整值多项式，则 $a_1,a_2,\cdots,a_{k+1}$都是整数。又 $a_0=p(n)-a_{k+1}\binom{n}{k+1}-a_k\binom{n}{k}-\cdots-a_1\binom{n}{1}$也是整数，因而 $p(x)$是整值多项式。

例 6 求证 $n\in Z,f(n)=\frac{1}{5}n^5-\frac{2}{3}n^2+\frac{13}{10}n-1$ 被 3 除余 2。

证明:要证 $f(n)\equiv 2(\mathrm{mod}\ 3)$，只需证 $f(n)+1\equiv 0(\mathrm{mod}\ 3)$也就是要证 $F(n)=\frac{f(n)+1}{3}$是整值多项式，由费尔马定理可证，下面用定理 6.8 来证。

$$F(n)=\frac{1}{15}n^5-\frac{1}{2}n^2+\frac{13}{30}n=n\left(\frac{1}{15}n^4-\frac{1}{2}n+\frac{13}{30}\right)$$

不难验证　$n=0,\pm1,\pm2$ 时，$\frac{1}{15}n^4-\frac{1}{2}n+\frac{13}{30}$的值都是整数，故 $\frac{1}{15}n^4-\frac{1}{2}n+\frac{13}{30}$是整值多项式，即说明 $F(n)$是整值多项式，从而此题得证。

2.2 欧拉(Euler)定理

定理 6.9 (欧拉定理)$m\geqslant2,(a,m)=1$

则 $a^{\varphi(m)}\equiv1(\mathrm{mod}\ m)$

证明：设 $r_1,r_2\cdots r_{\varphi(m)}$是模 m 的既约剩余系，由$(a,m)=1$ 知，$ar_1,ar_2\cdots ar_{\varphi(m)}$也是模 m 的既约剩余系，从而

$$\prod_{i=1}^{\varphi(m)}r_i\equiv\prod_{i=1}^{\varphi(m)}(ar_i)\pmod m$$

$$\prod_{i=1}^{\varphi(m)}r_i\equiv a^{\varphi(m)}\prod_{i=1}^{\varphi(m)}r_i\pmod m$$ 由于$(r_i,m)=1$，$i=1,2\cdots\varphi(m)$

故$(\prod_{i=1}^{\varphi(m)}r_i,m)=1$，则有 $a^{\varphi(m)}\equiv1(\mathrm{mod}m)$。

欧拉定理实际是费尔马定理的推广，因而应用更广泛。

例 1　设$(a,m)=1$，c 是使 $a^c\equiv1(\mathrm{mod}m)$成立的最小正整数，则 $c\mid\varphi(m)$。

证明：设 $c\nmid\varphi(m)$，则 $\varphi(m)=cq+r\quad 0<r<c$ 于是

$1\equiv a^{\varphi(m)}\equiv a^{cq+r}\equiv a^r(mod\ m)$这与 c 最小矛盾。

故必有 $c\mid\varphi(m)$。

定理 6.10　设$(a,m)=1$，d_0 是使 $a^d\equiv1(\mathrm{mod}m)$　　(8)

成立的最小正整数 d 的充要条件是 $a^{d_0}\equiv1(\mathrm{mod}m)$　　(9)

且 $a^0,a^1,\cdots a^{d_0-1}$　　(10)

对模 m 两两不同余。特别地，$d_0=\varphi(m)$的充要条件是(10)给出了模 m 的一组既约剩余系。

证明：先证定理的第一部分。设 d_0 是使(8)成立的最小正整数，即 $a^{d_0}\equiv1(\mathrm{mod}m)$。

若存在 $0\leqslant i<j\leqslant d_0-1$，使 $a^i\equiv a^j(\mathrm{mod}m)$

则 $a^i(a^{j-i}-1)\equiv0(\mathrm{mod}m)$,故 $a^{j-i}\equiv1(\mathrm{mod}m)$
而 $1\leqslant j-i<d_0$,这与 d_0 的最小性矛盾。

反之,若(10)给出了一组对模 m 两两不同余的数,且 $a^{d_0}\equiv1(\mathrm{mod}m)$,则由 $a^j\not\equiv a^0=1(\mathrm{mod}m)(j=1,2\cdots d_0-1)$,即当 $0<d<d_0$ 时,(9)式不成立,从而证明了 d_0 是最小的正整数。

再证第二部分。必要性由第一部分及 $\varphi(m)$ 的意义即得,充分性则由第一部分及欧拉定理保证。

例 2 若 1978^m 与 $1978^n(m>n\geqslant1)$ 的最后三位数字相同,试求 m,n,使 $m+n$ 的值最小。

证明: 依题意,应有 $1978^m-1978^n\equiv0\ (\mathrm{mod}1000)$

即 m,n 应同时满足下面两式

(ⅰ) $1978^m-1978^n\equiv0(\mathrm{mod}8)$ 即 $2^m989^m\equiv2^n989^n(\mathrm{mod}8)$

(ⅱ) $1978^m-1978^n\equiv0(\mathrm{mod}125)$ 即 $1978^{m-n}\equiv0(\mathrm{mod}125)$

由(ⅰ)可得:由于 $(8,989)=1$,故 $(989^m,8)=1$,从而有

$2^m989^{m-n}\equiv2^n(\mathrm{mod}8)$ 即 $2^n(2^{m-n}989^{m-n}-1)\equiv0(\mathrm{mod}8)$

显然 $(2^{m-n}989^{m-n}-1,8)=1$,故 $8|2^n$,从而 $n\geqslant3$,为使 $m+n$ 达到最小值,可取 $n=3$。

又由于 $(1978,125)=1,\varphi(125)=100$

由(ⅱ)可知 $m-n|100$,又由欧拉定理知 $1978^4\equiv1(\mathrm{mod}5)$ 由 $1978^{m-n}\equiv0(\mathrm{mod}125)$ 可知 $1978^{m-n}\equiv0(\mathrm{mod}5)$

当 $k=1,2,3$ 时,$1978^k\not\equiv1(\mathrm{mod}5)$,故 $4|m-n$,即 $m-n$ 只能是 4,20,100 三数之一,验证得到

$1978^4\equiv(-22)^4\equiv6(\mathrm{mod}125)$ $1978^{20}\equiv6^5\equiv31(\mathrm{mod}125)$

因此 $m-n$ 只能取 100,故 $m=103,n+m=106$。

例 3 正整数 M 取何值时,有 $5|(1999^M+M^{1999})$

解: 显然 $1999^M\equiv(-1)^M(\mathrm{mod}5)$。

当 $5|M$ 时,$M^{1999}\equiv0(\mathrm{mod}\ 5)$

当 $5\nmid M$ 时,由于 $\varphi(5)-4,(5,1999)-1,M^4\equiv1(\mathrm{mod}5)$

从而 $M^{1999}\equiv M^{4\times999+3}\equiv M^3(\mathrm{mod}5)$

设 $M=5k+r$，$r=1,2,3,4$ 时，M^3 除以 5 余数分别为 $1,-2,2,1$ 故当 $r=2,3$ 时，$5\nmid 1999^M+M^{1999}$

当 $r=1,4$ 时，对 M 的奇偶性进行讨论

若 M 为奇数，$1999^M\equiv-1(\text{mod}5)$，故只需 $M^{1999}\equiv1(\text{mod}5)$。

故 $M=5k+1$，又 M 是奇数，故 $M=10k+1\quad(k\in N)$。

若 M 为偶数，$1999^M\equiv1(\text{mod}5)$，只需 $M^{1999}\equiv-1(\text{mod}5)$

故 $M=5k+4$，且 k 偶数，故 $M=10k-1\quad(k\in N)$。

综上所述，当 M 为 1，11，21…或 9，19，29…时 $5\mid(1999^M+M^{1999})$。

2.3 威尔逊定理

定理 6.11 （威尔逊 wilson）

若 p 是素数，$r_1,r_2,\cdots r_{p-1}$是模 p 的既约剩余系，则

$$\prod_{r\bmod p} r=r_1r_2\cdots r_{p-1}\equiv-1(\text{mod}p)$$

特别地，即 $1,2,\cdots p-1$ 是模 p 的一组既约系，有

$$(p-1)!\equiv-1(\text{mod}p)$$

在证明定理之前，先看整数的一个有趣的性质。设 p 是素数，$1,2\cdots p-1$ 是模 p 的一组既约系，除去 1 和 $p-1$ 后剩下的 $p-3$ 个数两两结为一组，每一组数互为数论倒数。（若 $a\cdot a^*\equiv1(\text{mod}p)$，则称 a^* 是 a 的模 p 的数论倒数）。

例如 $p=7$，1，2，3，4，5，6 中去掉 1 和 6，其余 4 个数两两互为数论倒数，$2\times4\equiv1(\text{mod}7)$，$3\times5\equiv1(\text{mod}7)$。

证明：当 $p=2$ 时，定理成立。不妨设 $p\geqslant3$。由第五章知识知，对取定的 $r_1,r_2\cdots r_{p-1}$这一组既约系中的每个 r_i，必有唯一的 r_j，使得 $r_ir_j\equiv1(\text{mod}p)$ （11）

且 $r_i=r_j$ 的充要条件是 $r_i^2\equiv1(\text{mod}p)$ 即 $(r_i-1)(r_i+1)\equiv0(\text{mod}p)$。

由于 $p\geqslant3$ 是素数，故上式成立的充要条件是

$$r_i\equiv1(\text{mod}p)\text{或 }r_i\equiv-1(\text{mod}p) \qquad (12)$$

由于 $p\geqslant 3$，故上述两式不能同时成立。故在这组模 p 的既约系中，除了 $r_i\equiv 1, -1(\bmod p)$ 这两个数外，对其它的 r_i，必有 $r_j\neq r_i$，使(11)式成立。

不妨设 $r_1\equiv 1(\bmod p)$，$r_{p-1}\equiv -1(\bmod p)$，这样在这组模 p 的既约系中除式满足(12)式的两数外，其余的数恰好按(11)式两两配对，即有 $r_2, r_3\cdots r_{p-2}\equiv 1(\bmod p)$。，故有 $r_1, r_2\cdots p_{p-1}\equiv -1(\bmod p)$。当取 $1,2,\cdots p-1$ 为模 p 的既约系时，显然有 $(p-1)!\equiv -1(\bmod p)$ 威尔逊定理得证。

数学竞赛中经常用到威尔逊定理的特殊情况，即 $(p-1)!\equiv -1(\bmod p)$，其逆也真，即有下述定理。

定理 6.12　若 $(p-1)!\equiv -1(\bmod p)$，则 p 为素数。

证明：假设 p 不是素数，则存在 d，$d\mid p$ 且 $1<d<p$，

由 $(p-1)!\equiv -1(\bmod p)$ 及 $d\mid p$ 得

$(p-1)!\equiv -1(\bmod d)$　但由于 $d<p$，故 $d\mid(p-1)!$

从而 $0\equiv -1(\bmod d)$，矛盾，故 p 为素数。

威尔逊定理及其逆给出了确定素数的充要条件，即一个整数 $m>1$ 是素数的充分必要条件是 $(m-1)!\equiv -1(\bmod m)$。下面说明威尔逊定理在二次同余式上的应用。

例 1　若 p 是大于 2 的素数，则

$$\left(\frac{p-1}{2}!\right)^2+(-1)^{\frac{p-1}{2}}\equiv 0(\bmod p)$$

证明：小于 p 的正整数可写成

$1,2,\cdots\frac{p-1}{2}, p-\frac{p-1}{2},\cdots p-2, p-1$，故

$$\begin{aligned}(p-1)! &= 1\times 2\times\cdots\times\frac{p-1}{2}\times\left(p-\frac{p-1}{2}\right)\times\cdots(p-2)(p-1)\\ &= 1\times 2\times\cdots\times\frac{p-1}{2}\times(p-1)(p-2)\cdots\left(p-\frac{p-1}{2}\right)\equiv(-1)^{\frac{p-1}{2}}\left(\frac{p-1}{2}!\right)^2(\bmod p)\end{aligned}$$

由威尔逊定理知$(-1)^{\frac{p-1}{2}}\left(\frac{p-1}{2}!\right)^2\equiv -1(\bmod p)$

$$即\left(\frac{p-1}{2}!\right)^2+(-1)^{\frac{p-1}{2}}\equiv 0(\bmod p)$$

例 2 二次同余式 $x^2+1\equiv 0(\bmod p)$有解的充分必要条件是 $p\equiv 1(\bmod 4)$,其中 p 是奇素数。

证明:充分性:若 $p\equiv 1(\bmod 4)$,则

$(p-1)!=1\times 2\times\cdots\times\frac{p-1}{2}\cdot(p-1)(p-2)\cdot\left(p-\frac{p-1}{2}\right)\equiv(-1)^{\frac{p-1}{2}}\left(\frac{p-1}{2}!\right)^2(\bmod p)$

故 $-1\equiv(p-1)!\equiv\left(\frac{p-1}{2}!\right)^2(\bmod p)$

即$\left(\frac{p-1}{2}!\right)$满足二次同余式 $x^2+1\equiv 0(\bmod p)$

必要性:

设 a 是 $x^2+1\equiv 0(\bmod p)$的任一解,因而 $a^2\equiv -1(\bmod p)$
由 $p\nmid a$ 及费尔马定理知

$$1\equiv a^{p-1}=(a^2)^{\frac{p-1}{2}}\equiv(-1)^{\frac{p-1}{2}}(\bmod p)$$

故 $p\mid(1-(-1)^{\frac{p-1}{2}})$,若 $1-(-1)^{\frac{p-1}{2}}\neq 0$,则 $p\mid 2$,这与 p 是奇数矛盾,于是有 $1=(-1)^{\frac{p-1}{2}}$,即$\frac{p-1}{2}$为偶数,故 $p\equiv 1(\bmod 4)$。

由此题知 $x^2+1\equiv 0(\bmod 17)$的解为$\frac{n-1}{2}!=8!\equiv 13(\bmod 17)$

即 $x^2+1\equiv 0(\bmod 17)$的解为 $x\equiv 13(\bmod 17)$

例 3 设 p 是奇素数,证明

(1) $1^2\times 3^2\times 5^2\times\cdots\times(p-2)^2\equiv(-1)^{\frac{p+1}{2}}\quad(\bmod p)$

(2) $2^2\times 4^2\times 6^2\times\cdots\times(p-1)^2\equiv(-1)^{\frac{p+1}{2}}\quad(\bmod p)$

证明:由于 $k\equiv -(p-k)\quad(\bmod p)$,依次令 $k=1,3,5\cdots$

$(p-2)$，得

$$1 \equiv -(p-1) \pmod{p}$$
$$2 \equiv -(p-2) \pmod{p}$$
$$\vdots$$
$$\vdots$$
$$(p-2) \equiv -(p-(p-2)) \pmod{p}$$

两边分别相乘得

$$1\times 3\times 5\times\cdots\times(p-2)\equiv[-(p-1)][-(p-3)]\times\cdots\times[-2] \pmod{p}$$

$$1\times 3\times 5\times\cdots\times(p-2)\equiv(-1)^{\frac{p-1}{2}}[2\times 4\times 6\times\cdots\times(p-1)] \pmod{p}$$

两边都乘以 $1\times 3\times 5\times\cdots\times(p-2)$ 得

$$1^2\times 3^2\times\cdots\times(p-2)^2\equiv(-1)^{\frac{p-1}{2}}(p-1)!\equiv(-1)^{\frac{p+1}{2}} \pmod{p}$$

这就证明了(1)，仿(1)可证(2)。

例 4 设 $r_0,r_1\cdots r_{p-1}$ 及 $r'_0,r'_1\cdots r'_{p-1}$ 是模 p 的两组完全剩余系，p 是奇素数，证明：$r_0r'_0,r_1r'_1\cdots r_{p-1}r'_{p-1}$ 一定不是模 p 的完全剩余系。

证明：采用反证法。假设 $r_0r'_0,r_1r'_1\cdots r_{p-1}r'_{p-1}$ 是模 p 的一组完系，则其中有且仅有一个被 p 整除，不妨设 $p\mid r_0r'_1$，$p\nmid r_ir'_i$　$i=1,2\cdots p-1$ 因而必有 $p\mid r_0$，$p\mid r'_0$，$p\nmid r_i$，$p\nmid r'_i$　$i=1,2\cdots p-1$。

故 $r_1,r_2\cdots r_{p-1}$ 及 $r'_1,r'_2\cdots r'_{p-1}$ 都是模 p 的既约系，故 $r_1r'_1$，$r_2r'_2\cdots r_{p-1}r'_{p-1}$ 也是模 p 的一组既约系，故由威尔逊定理知

$$r_1r_2\cdots r_{p-1}\equiv -1 \pmod{p}$$
$$r'_1r'_2\cdots r'_{p-1}\equiv -1 \pmod{p}$$

$$(-1)(-1)\equiv(r_1\cdot r'_1)(r_2\cdot r'_2)\cdots(r_{p-1}r'_{p-1})\equiv -1 \pmod{p}$$

由 $p>2$　则 $-1\not\equiv 1 \pmod{p}$ 故假设不成立，命题得证。

练 习 二

1. 今天是星期一，问再过 $38^{35^{39}}$ 天是星期几？

2. 证明：若 $p.q$ 均为奇素数，且 $(p,q-1)=1$，$(q,p-1)=1$，则 $(p-1)^{q-1}\equiv(q-1)^{p-1}\pmod{pq}$。

3. 证明 $f(x)=\frac{1}{5}x^5+\frac{1}{3}x^3+\frac{7}{15}x$ 为整值多项式。

4. 确定正整数 n，使 $5^{2n}+3^{2n}\equiv0\pmod{17}$。

5. 设 p 是素数，$(a,p)=1$，则(1)当 a 为奇数时，$a^{p-1}+(p-1)^a\equiv0\pmod p$

(2)当 a 为偶数时，$a^{p-1}-(p-1)^a\equiv0\pmod p$。

6. 若 $p>3$，p 是素数，证明 $42p\mid3^p-2^p-1$。

7. 若 m,n 为自然数，$m>n$，当 4^m+4^n 为 100 的倍数时，$m+n$ 的最小值是多少？

8. 一个 $6n$ 位数能被 7 整除，将最末位数字移到首位得到一个数，则此数也能被 7 整除。

9. 证明：若 $p=4n+1$，则 $\left(\frac{(4n)!}{(2n)!}\right)^2+1\equiv0\pmod n$。

10. p 为素数，试证：任意的 $2p-1$ 个自然数可选出 p 个数，使其和被 p 整除。

11. 若一个正整数的十进位表示是由一个(不从 0 开始的)数字块及紧跟在其后的完全相同的块组成如 286286，称这个数为二重数。证明有无穷多个二重数是完全平方数。

12. 试求所有的正整数 $n>1$，使得 $\frac{2^n+1}{n^2}$ 是整数。

第七章　专题选讲

§1　枚举与筛选

1.1　有关概念

我们在分析和解决问题时，特别是复杂的问题，常把要讨论的对象分成若干种情况，即先把解决问题的各种可能性一一列举出来，再根据问题的条件逐一讨论，逐次淘汰各种无解的可能，从而求出解答。

例如讨论有关自然数的问题时，可以将自然数一一列举，1、2、3、4…；也可以按奇偶分类；还可以按模 m 的剩余类分类……。在讨论有关三角形的问题时，可以将三角形分为锐角三角形、直角三角形、钝角三角形。

根据情况一一列举并逐一讨论，这种解决问题的方法就是枚举法，也称列举法或分类法。

枚举的原则是既不能重复也不能遗漏。

枚举法是一种很简单又很实用的方法。在面临复杂情况，无法整体处理时，常常采用枚举法。

在运用枚举法求解问题时，我们希望尽量缩小枚举的范围，使枚举的情况越少越好，这就是筛选法。这样可以避免不加分析地列举而精疲力尽事倍功半。

例如寻找 50 以内全部素数，我们就可以用枚举、筛选法。首先列出 1～50，然后删去 1 和所有 2 的倍数（把 2 留下）；再把 2 后面第一个未划去的素数 3 留下，删去所有 3 的倍数；再把 3 后面未划去的素数 5 留下，删去所有 5 的倍数，继续下去，最后列出了 50 以内的素数。

~~1~~ 2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~
~~16~~ 17 ~~18~~ 19 ~~20~~ ~~21~~ ~~22~~ 23 ~~24~~ ~~25~~ ~~26~~ ~~27~~ ~~28~~
29 ~~30~~ 31 ~~32~~ ~~33~~ ~~34~~ ~~35~~ ~~36~~ 37 ~~38~~ ~~39~~ ~~40~~ 41
~~42~~ 43 ~~44~~ ~~45~~ ~~46~~ 47 ~~48~~ ~~49~~ ~~50~~

这种寻找素数的方法通常叫 Eratoschenes 筛法

1.2 基本方法与技巧

例 1 六条棱长分别是 2,3,3,4,5,5 的所有四面体中,最大的体积是多少?

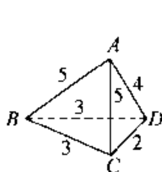
解: 以 2 为一边的三角形有四种可能的情形:

(1)2,3,3 (2)2,3,4 (3)2,4,5 (4)2,5,5

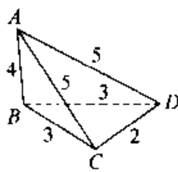
在四面体的四个面中,棱长是 2 的面有两个,这两个面有下列三种情形:

(a) (2,3,3)和(2,4,5) (b) (2,3,3)与(2,5,5) (c) (2,3,4) (2,5,5)

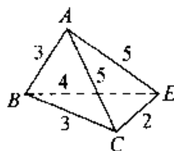
故构成的四面体分别是



(A)



(B)



(C)

与(a),(c)两种情形对应的图形各有两种,但因两个图形的体积相同,故只画出了相应的一种图形。

易知 $V_A=\frac{1}{3}\cdot h_1\cdot S_{\triangle BCD}<\frac{4}{3}\cdot S_{\triangle BCD}=V_B$

$$V_B=\frac{1}{3}\cdot AB\cdot S_{\triangle BCD}=\frac{4}{3}\cdot S_{\triangle BCD}=\frac{8}{3}\sqrt{2}$$

$$V_C=\frac{1}{3}\cdot h_2\cdot S_{\triangle BCD}<S_{\triangle BCE}=\frac{3}{4}\sqrt{15}<\frac{3}{4}\sqrt{16}=3<\frac{8}{3}\sqrt{2}$$

故所求体积的最大值是$\frac{8}{3}\sqrt{2}$。

例 2 设 p 是大于 3 的奇素数,证明:p^2-1 必能被 24 整除。

解:$p^2-1=(p+1)(p-1)$ 由 p 是奇数知 $4|(p^2-1)$,下面只要证明 $6|(p^2-1)$ 即可,我们考虑 p 模 6 的同余类。$6n$,$6n\pm1$,$6n\pm2$,$6n+3(n\in N)$

由于 $6n+3$,$6n\pm2$,$6n$ 都是合数,因此只考虑 $p=6n\pm1$ 型的数。

令 $p=6n\pm1$,则 $p^2-1=12n(3n\pm1)$,显然 $6|(p^2-1)$

即当 $p=6n\pm1$ 时,p^2-1 都能被 24 整除,而 $6n\pm1$ 型的数包含了所有大于 3 的素数。

例 3 A、B、C 三人作下列游戏:在三张卡片上分别写上整数 $p,q,r(0<p<q<r)$。把这三张卡片混合后分发给 A、B、C 三人,每人各得一张,再按各人所得卡片上的数字,发给小球,然后将卡片收回,但分得的球留给各人,如此进行若干轮(每轮包括混合卡片,发卡片,发球和收卡片),最后一轮结束后,A,B,C 三人分得 20,10,9 个球,还知道 B 在最后一轮游戏得了 r 个球。问谁在第一轮得到了 q 个球?

解:设游戏进行了 k 轮,则

$$k(p+q+r)=20+10+9=39=3\times13$$

由于 $0<p<q<r$, $p+q+r\geqslant6$, $k\geqslant2$,

故 $k=3,p+q+r=13$。

由于 B 最后一轮得 r 个球,但总数小于 B,所以他在第一轮、第二轮每轮都得到 p 个球,即

$$p+p+r=10$$

由于 C 所得球的总数小于 10,因此他没有一轮得 r 个球,同时 B 第一轮已经得了 p 个球,所以只有 C 在第一轮得 q 个球。

	A	B	C
第一轮	r	p	q
第二轮	r	p	r
第三轮	q	r	p
合计	20	10	9

由上表可以求出 $r=8,q=4,p=1$。

例 4 给定一个整数 $n_0>1$ 后，两名选手 A、B 按以下规则轮流取整数 $n_1,n_2,n_3\cdots$

在已知 n_{2k} 时，选手 A 可以取任一整数 n_{2k+1}，使得 $n_{2k}\leqslant n_{2k+1}\leqslant n_{2k}^2$

在已知 n_{2k+1} 时，选手 B 可以取任一整数 n_{2k+2}，使得 $\frac{n_{2k+1}}{n_{2k+2}}$ 是一个质数的正整数幂。

若 A 取到 1990，则 A 胜；若 B 取到 1，则 B 胜。

对怎样的初始值 n_0，

（ⅰ）A 有必胜策略。

（ⅱ）B 有必胜策略。

（ⅲ）双方均无必胜策略？

解：$n_0=2$ 时，A 取 n_1，$2\leqslant n_1\leqslant 2^2$，故 A 可取 2，3，4，B 可取 1，B 胜。

$n_0=3$ 时，A 可取 3～9，均为形如 p^k 或 $2p^k$（p 为质数）的数，从而 B 可取 1 或 2，B 胜。

$n_0=4$ 时，A 可取 4～16，均为形如 p^k，$2p^k$ 或 $3p^k$ 的数，从而 B 可取 1，2 或 3，B 胜。

$n_0=5$ 时，A 可取 5～25，均为形如 p^k，$2p^k$，$3p^k$ 或 $4p^k$ 的数，从而 B 可取 1，2，3，4，B 胜。

若 $44\leqslant n_0\leqslant 1990$，则 A 可取 1990，A 胜。

若 $21\leqslant n_0\leqslant 43$ 则 A 可取 $420=2^2\times 3\times 5\times 7$，$B$ 取的数在 44～1990 之间，则由前一种情况，A 胜。

若 $13\leqslant n_0\leqslant 20$，则 A 可取 $168=2^3\times 3\times 7$，B 取的数在 21～1990 之间，故 A 胜。

$11\leqslant n_0\leqslant 12$，则 A 可取 $105=3\times 5\times 7$，B 取的数在 13～1990 之间，A 胜。

$8\leqslant n_0\leqslant 10$，则 A 取 $60=2^3\times 3\times 5$，B 取的数在 12～1990 之

间,A 胜。

若 $n_0>1990$,A 取 $n_1=2^{r+1}\times3^2$,满足

$2^r\times3^2<n_0\leqslant2^{r+1}\times3^2<n_0^2$

则 n_2 满足 $8\leqslant n_2\leqslant n_0$,用 n_2 代替 n_0,继续采取上面的方法,经过有限步后得到

$$8\leqslant n_{2k}<1990 \quad \text{于是 } A \text{ 胜。}$$

最后,在 $n_0=6$ 或 7 时,A 取 $n_1=30$,则 B 只可取 6,(因若 B 取 10 或 15,A 均胜),A 再取 30,这样 A 立于不败之地。

另一方面,在$\leqslant7^2$ 的数中,A 只有取 30 与 42,才能保证 $n_2\geqslant6$,(否则 $n_2\leqslant5$,B 胜),此时 B 总可以取 6,因此 B 可立于不败之地。

所以当 $n_0=6$ 或 7 时,两人均无必胜策略。

在本例中有无穷多个自然数要讨论,如果没有枚举的思想,只会盲目地分类,既费时间,又有可能重复或遗漏。由此也可以看出,枚举与筛选虽然是一种极基本的方法,但却是非常重要的。

例 5 从 1,2,3…1998,1989 中任意选取 k 个数,使得在所选的 k 个数中一定可以找到能构成一个三角形边长的三个数。试问满足上述条件的 k 的最小值是多少?

解: 从{1,2,3…1988,1989}中,按递推公式 $a_1=1,a_2=2$,$a_{n+2}=a_{n+1}+a_n$ 选取出 16 个数{1,2,3,5,8,13,21,34,55,89,144,233,377,610,987,1597}。其中的任意三个数,都不能构成三角形。故 $k\geqslant17$。

下面说明 $k=17$ 时,总可以找到能构成三角形的三个数。

设 $a_1<a_2<\cdots<a_{17}$是从{1,2,……1989}中任意选取的某 17 个数,若这 17 个数中不存在能构成三角形的三个数,则有

$a_1\geqslant1,a_2\geqslant2,a_3\geqslant a_1+a_2\geqslant3 \quad a_4\geqslant a_2+a_3\geqslant5\cdots\cdots$

$a_{16}\geqslant a_{14}+a_{15}\geqslant1597,a_{17}\geqslant a_{15}+a_{16}\geqslant2584$,这与 $a_{17}\leqslant1989$ 矛盾。这说明从{1,2…1989}中任意选取 17 个数,总可以找到能构成三角形的三个数。故 k 的最小值是 17。

抽屉原理(也叫逐步淘汰原理)是一种很有用的枚举与筛选的方法。我们都知道,任选 13 个人,其中必有两人具有相同的属相。用枚举的方法很容易说明这一事实。

例 6 有 6 个代表队共 1958 名运动员,编上号码 1,2,…1958。证明至少有一个运动员的号码等于他的两个队友的号码的和或者等于一个队友的号码的 2 倍。

证明:不妨设第 1 个代表队人数最多,它的人数$\geqslant\left[\frac{1958}{6}\right]+1=327$。设其中最大的号码是 a_1,用 a_1 减其它 326 个队友的号码,得到的差如果仍是第 1 个代表队队员的号码,则结论成立。

如果这 326 个差 a_1-a_j 都不在第 1 个代表队中,那么不妨设 $\left[\frac{326}{5}\right]+1=66$ 个在第 2 代表队中同样设最大的号码为 b_1,用 b_1 减其它 65 个号码

$$b_1-b_i=(a_1-a_s)-(a_1-a_t)=a_t-a_s$$

如果这差在第 1 或第 2 代表队中结论成立。

设这 65 个差不在第 1 或第 2 代表队中,继续考虑$\left[\frac{65}{4}\right]+1=17$,$\left[\frac{16}{3}\right]+1=6$,$\left[\frac{5}{2}\right]+1=3$ 项的差,或者结论成立,或者最后得到两个号码在第 6 个代表队中,而这两个号码的差形如

$a_t-a_s=b_j-b_i=c_n-c_m=d_p-d_q=e_k-e_h$。无论属于哪个代表队,结论均成立。

练 习 一

1. 已知四位数$\overline{abcd}$是 11 的倍数，$b+c=a$，且两位数$\overline{bc}$是完全平方数，求此四位数。

2. 将 2000 分拆成自然数之和，$2000=a_1+a_2+\cdots$，再将 a_1，a_2，$a_3\cdots$相乘，求所有这种乘积中的最大值。

3. 假设 a_1,b_1,c_1,a_2,b_2,c_2 是这样的实数，使得对于任何整数 x 和 y，数

$a_1x+b_1y+c_1$ 和 $a_2x+b_2y+c_2$ 中至少有一个是偶数值。

证明：两组系数 a_1,b_1,c_2 和 a_2,b_2,c_2 中至少有一组全是整数。

4. 已知自然数 a 共有 10 个正约数，且 $a<100$，求 a。

5. 最大的不能写成两个奇合数之和的偶数是几？

6. 有五名学生 A,B,C,D,E 参加一次竞赛，某人猜测竞赛结果的名次是 $ABCDE$，但既没有猜中任何名次，也没有猜中任何一对相邻名次的顺序，另一人猜测的名次是 $DAECB$，这人猜中了两个名次，还猜中了两对相邻名次的顺序，求竞赛结果的实际名次。

7. 黑板上开始写有 3 个自然数，擦去其中任一个数，改成另二数和减去 1 的数，反复这样进行，在某时刻黑板上出现了 17，1967，1983 这三个数，问最初写在黑板上的三个数能否是 2，2，2 或 3，3，3？

8. 任意 10 个整数 $a_1,a_2\cdots a_{10}$。试证：必存在一个非零数组 $(x_1,x_2\cdots x_{10})$，$x_i\in\{-1,0,1\}$，使得

$$1001\mid\sum_{i=1}^{10}x_ia_i$$

9. 直三棱柱棱长的数值均为质数，且唯一的最短棱是底面棱，这个三棱柱侧面积恰为 1984。试计算这个三棱柱的体积。

10. 有 17 个同学参加关于小论文 A、B、C 的讨论会，试证：其中至少有 3 个同学彼此讨论的内容是同一篇论文。

§2 集合、分划与整数分拆

2.1 概念

集合、分划与整数分拆是联系非常密切的两类问题，在国内外各级数学竞赛中，这类问题经常出现。例如为了方便讨论问题，经常把整数集分成奇数和偶数两类，即按模 2 的同余类分类。另外，最简单的二元一次不定方程 $ax+by=c$，$(a,b,c\in N)$，有整数解的充要条件是 $(a,b)\mid c$。这也说明了若此方程有整数解，则 c 可以写成若干个自然数 a 与若干个自然数 b 的和。这两类问题涉及到许多基础知识，如整数性质，分类思想，构造意识，计数知识，排序原理，确界思想，映射等等，是数学竞赛中比较灵活的问题。

定义 7.1 设 $S_1,S_2\cdots\cdots S_k$ 是集合 X 的非空子集，如果

(1) $S_i\cap S_j=\phi(i\neq j)$

(2) $X=S_1\cup S_2\cup\cdots\cup S_k$

则称 $S_1,S_2\cdots S_k$ 是 X 的一个 k - 分划，其中 k 叫做分划的长度，S_i 叫做分划的部分；如果 $S_1,S_2\cdots S_k$ 只满足条件(2)，则称 $S_1,S_2\cdots S_k$ 是集合 X 的一个 k - 覆盖。

例如，集合 $X=\{a,b,c,d\}$ 的 3 - 分划共有 6 个，分别是：

$(\{a,b\},\{c\},\{d\})$； $(\{a,c\},\{b\},\{d\})$

$(\{a,d\},\{b\},\{c\})$； $(\{b,c\},\{a\},\{d\})$

$(\{b,d\},\{a\},\{c\})$； $(\{c,d\},\{a\},\{b\})$

一般，我们讨论 n 元有限集 $X=\{a_1,a_2\cdots a_n\}$。X 有两个特殊的分划，即 $X=X$ 是一个 1 - 分划而 $X=\{a_1\}\cup\{a_2\}\cup\cdots\cup\{a_n\}$ 是一个 n - 分划，X 其余的 k - 分划都满足 $1<k<n$。我们用 $P(x,k)$ 表示 n 元集合 X 的 k - 分划总数，用 $P(x)$ 表示 n 元集合 X 所有分划的总数，则有 $P(x,1)=P(x,n)=1$，$P(x)=\sum\limits_{k=1}^{n}P(x,k)$。

集合分划是经常用到的，分划的原则必须不重复不遗漏，即把

全集分成若干个不相交的子集的并，因此，从数量上看，全集的元素个数($x=\{a_1,a_2,a_3,\cdots a_n\}$)正好是各子集元素个数之和，即 $|x|=\sum_{i=1}^{k}|S_i|$，不妨设 $|S_i|=n_i$　$i=1,2\cdots k$，则有 $n=n_1+n_2+\cdots n_k$，即自然数 n 可以写成 k 个自然数之和，这也反映了集合分划与整数分拆之间的联系。

定义 7.2　设 n 是自然数，将 n 写成 k 个自然数之和，即 $n=n_1+n_2+\cdots+n_k$，其中 $1\leqslant k\leqslant n$，$n_1\geqslant n_2\geqslant n_3\geqslant\cdots\geqslant n_k\geqslant 1$，称 $n_1,n_2,\cdots,n_k$ 是 n 的一个 k-分拆，k 叫做分拆的长度，n_i 叫分拆的项。

自然数 n 的不同 k-分拆的总数记作 $p(n,k)$；

n 的所有分拆的总数记作 $p(n)$。

$p(n)=\sum_{k=1}^{n}p(n,k)$

例 1　把集合 $M=\{1,2\cdots 2n\}(n\in N)$ 任意分成子集合 A，B，$A\cap B=\phi$，$A\cup B=M$。且 $|A|=|B|=n$。
设 $A=\{a_1,a_2\cdots a_n\}$，$B=\{b_1,b_2\cdots b_n\}$ 且 $a_1<a_2<\cdots<a_n$，$b_1>b_2\cdots>b_n$。证明：

$|a_1-b_1|+|a_1-b_2|+\cdots+|a_n-b_n|=n^2$

分析： 考虑 $M_1=\{1,2\cdots n\}$，$M_2=\{n+1,n+2\cdots 2n\}$
如果 $a_1=n+1$，则 $A=M_2$，$B=M_1$。此时

$|a_1-b_1|+|a_2-b_2|+\cdots+|a_n-b_n|=|(n+1)-n|+|n+2-(n-1)|+\cdots+|2n-1|=n^2$

如果 $a_1\leqslant n$，则 $a_1\in M_1$，$b_1\in M_2$，这说明 A 中最小元素与 B 中最大元素不同在 M_1，M_2 中，即 a_1，b_1 这两个数一个在 M_1 中，一个在 M_2 中，同样的分析又知 a_i，b_i 这两个数一个在 M_1 中，另一个在 M_2 中。

解： 设 M_1，M_2 是 M 的任一分划。则 a_i，b_i，$i=1,2\cdots n$ 不同在 M_1 或 M_2 中，则

$$\sum_{i=1}^{n}|a_i-b_i|=[(n+1)+(n+2)+\cdots+2n]-(1+2+\cdots+n)=n^2$$

例2 对于集合$\{1,2,\cdots,n\}$及其任一非空子集定义“交替和”如下:按递减顺序重排这个集合中的元素,然后从最大的元素开始交错减、加后边的数,所得的结果叫这个集合的交替和。例如$\{1,2,0,-3,5\}$的交替和是$5-2+1-0+(-3)=1$,求集合$\{1,2,\cdots n\}$及其全部非空子集的交替和的总和。

解:$\{1,2\cdots,n\}$的非空子集共有$C_n^1+C_n^2+\cdots+C_n^n=2^n-1$个,补上一个不影响交替和的集合$\{0\}$,按以下方式两两结为一组:

$\{n\}$与$\{0\}$为一组,　　$\{1,n\}$与$\{1\}$为一组;

$\{2,n\}$与$\{2\}$为一组,……,$\{n-1,n\}$与$\{n\}$为一组;

$\{1,2,n\}$与$\{1,2\}$为一组,……

$\{1,2,\cdots n-1,n\}$与$\{1,2\cdots n-1\}$为一组

易知每一组中的两个子集交替和的和为n,由于共有2^{n-1}组,则集合$\{1,2\cdots n\}$及其全部非空子集的交替和的总和是$n\cdot 2^{n-1}$。

例3 整数9可表成两个连续整数的和,$9=4+5$,同时,它恰可用两种不同的方法写成连续整数和:$9=4+5=2+3+4$。
是否有这样的整数,它可以表成1990个连续整数的和,并且恰有1990种不同的方法表成连续整数和。

解:设$m=n_0+(n_0+1)+(n_0+1989)$且$M=n+(n+1)+\cdots+(n+k)$恰有1990对不同的(n,k)。

则　$m=1990n_0+\dfrac{1990\times1989}{2}=\dfrac{1990}{2}(2n_0+1989)$

$2m=(k+1)(2n+k)$,除去$1,2m$外,$2m$还有1990对不同的因数。

令$n_0=\dfrac{5^9\cdot199^{179}-1989}{2}$,则$m=5^{10}\times199^{180}$

$2m=2^1\times5^{10}\times199^{180}$共有$(1+1)\times(10+1)\times(180+1)=2\times1991$个因数。

将因数 a 与 $b=\frac{2m}{a}$ 配对，去掉 $(1,2m)$，剩下 1990 对，每一对因数 (a,b) 对应一组 (n,k)。

设 $b>a$，则 $k=a-1$，$n=\frac{b-a+1}{2}$。由于 a,b 中(即 $k+1$，$2n+k$)恰有一个是偶数，故 $n\in N$。反之，每一组 (n,k) 对应一对因数 (a,b)。故 $5^{10}\times 199^{180}$ 可以表成 1990 个连续整数的和，并且恰有 1990 种不同的方法表成连续整数的和。

2.2 基本方法

如果有限集 X 可以分拆成 $A_1,A_2\cdots A_k$，k 个子集的并，则 A 中元素的个数等于 $\sum_{i=1}^{k}|A_i|$，即对集合 X 的计数问题可以转化到 k 个不交的较易计数的 k 个子集上。解决计数问题并不容易，假定所要计数的集合 A 很复杂，除了将 A 分拆成较易计数的子集外，还可以寻找一个便于计数的集合 B，并且建立集合 A 到 B 上的双射 f，这样就将求 $|A|$ 的问题转移到易求的 $|B|$。即配对法，或称配对原理。

设 A 和 B 为有限集合，f 是 A 与 B 之间的双射，则集合 A 与集合 B 的元素个数相等，即 $|A|=|B|$。

例 1 证明自然数 n 的分拆数 $P(n,k)$ 满足递推关系 $P(n+k,k)=P(n,1)+P(n,2)+\cdots+P(n,k) \quad 1\leqslant k\leqslant n$。

证明 $P(n+k,k)$ 是指 $n+k$ 的 $k-$分拆总数

$\sum_{i=1}^{k}P(n,i)$ 是指 n 的长度不超过 k 的分拆总数。

对 $n+k$ 的任意一个 $k-$分拆

$$n+k=n_1+n_2+\cdots+n_k \qquad n_i\geqslant 1 \quad i=1,2\cdots k$$

即 $n=(n_1-1)+(n_2-1)+\cdots+(n_k-1) \qquad n_i-1\geqslant 0 \quad i=1,2,\cdots,k$

总对应着 n 的一个长度不超过 k 的分拆。

同理，n 的任意一个长度不超过 k 的 $m-$分拆，

设 $n = n_1 + n_2 + \cdots + n_m + \underbrace{0 + \cdots + 0}_{k-m\text{个}0} \quad m \leqslant k$

即 $n + k = (n_1 + 1) + (n_2 + 1) + \cdots + (n_m + 1) + \underbrace{1 + 1 + \cdots + 1}_{\text{共}k-m\text{个}1}$

即 $n + k$ 有一个 k－分拆与 $n = n_1 + n_2 + \cdots + n_m$ 对应，易证这种对应是一一的，故 $P(n+k,k) = \sum_{i=1}^{k} P(ni)$

例 2 给定格点 $P(a_0,b_0)$ 与 $Q(a,b)$ $a > a_0$，求连结 P 与 Q 的折线的条数。

在正方形网格上，从某个格点 $P_0(a_0,b_0)$ 出发，向右画一条斜率为 1 或者 −1 的线段，其右端点为 $P_1(a_1,b_1)$，其中 $a_1 = a_0 + 1$，$b_1 = b_0 \pm 1$，再从格点 P_1 出发，向右画一条斜率为 1 或者 −1 的线段，其右端点为 $P_2(a_2,b_2)$，$a_2 = a_0 + 2$，$b_2 = b_1 \pm 1$，等等，经过 n 步，一直画到格点 $P_n(a_n,b_n)$，其中 $a_n = a_0 + n$，$b_n = b_{n-1} \pm 1$，得到一条折线。各方格中出现折线 L 的那一段叫做折线 L 的一节。

解 所有连结格点 P 与 Q 的折线的集合记作 S。设 $L \in S$，$n = a - a_0$。则折线 L 由 P 到达 Q 必须经过 n 步，即折线 L 由 n 节组成。设其中向上的共有 x 节，向下的有 y 节，则 $x - y = b - b_0$ $x + y = n$。即 $x = \frac{n + (b - b_0)}{2}$，$\frac{a - a_0 + b - b_0}{2} = n_1$ $a - a_0 + b - b_0$ 是偶数时，n_1 是整数，折线 L 存在。现在取编号 1，2 $\cdots n$ 的 n 个空格，如果折线 L 自左至右算起的第 i 节是向上的，则在第 i 个空格里填上 1，否则填上 0，$i = 1,2\cdots n$，得到将 n_1 个 1 与 $n - n_1$ 个 0 填到 n 个空格的一种填法将所有 n_1 个 1 与 $n - n_1$ 个 0 填进 n 个空格的填法的集合记作 T。每一折线 $L \in S$，就有一种填法 $f(L) \in T$ 与之对应，建立 S 到 T 的映射，易证 f 是双射，故 $|S| = |T| = C_n^{n_1}$。

例 3 将正整数 m 写成 n 个正整数的和，如果加数的位置不同，也认为是不同的写法。求有多少种不同的写法。

$m=x_1+x_2+\cdots+x_n, x_i\in N$,如果 $x_1\geqslant x_2\geqslant\cdots\geqslant x_n$,这种分拆是不考虑顺序的,通常称为无序分拆。如果考虑顺序,即加数的位置不同,也认为是不同的写法,则称为有序分拆。例如 $5=3+2=2+3$ 认为是两种不同的 2-分拆。

解:设 $m=x_1+x_2+\cdots+x_n, x_i\in N, i=1,2\cdots,n$。

则 $(x_1-1)+(x_2-1)+\cdots+(x_n-1)=m-n$。 其中 $x_i-1\geqslant 0, i=1,2\cdots,n$。

设有 n 个盒子,将 $m-n$ 个球分配给 n 个盒子,即从 n 个中选 $m-n$ 个允许重复的组合数 $C_{n+(m-n)-1}^{m-n}$ 就是分配的方式,故共有 C_{m-1}^{n-1} 种分配方式,显然 $x_1,x_2\cdots x_n$ 的每一种不同的顺序对应一种球的放法,而且这种对应是一一对应的,故 m 的有序 n-分拆有 C_{m-1}^{n-1} 种方法。

例 4 将集 $\{1,2\cdots,n\}$ 分拆为三个互不相交的子集 A_1,A_2,A_3,(其中允许有空集)满足:

(1) 若每个子集的元素依递增次序排列,则相邻的元素奇偶性不同。

(2) 若 A_1,A_2,A_3 均非空,则其中恰有一个集合的最小元素是偶数。

求这种分拆的个数。

解:不妨设 $1\in A_1$,A_2 的最小元小于 A_3 的最小元,显然 2 有两种放法:放入 A_1 或 A_2。

设小于 k 的数均有两种可能的放法,并已放妥,现在考虑 k,这时有以下三种情况:

(ⅰ) A_2,A_3 中均未放元素,则 k 可以放入 A_1 或 A_2,不能放入 A_3 中。

(ⅱ) A_2 中已有元素,A_3 中还没有元素,则 k 可以放入 $k-1$ 所在的集合,不妨设为 A_1 中;同时 $k-1$ 还可以放入 A_2 或 A_3 中,如果 $k-1$ 可以放入 A_3 中,则 $k-1$ 与 A_2 的最小元素奇偶性不同,故 k 与 A_2 的最小元素奇偶性相同,不能放入 A_3 中,但这时

$k-1$ 不能放入 A_2 中，故 k 能放入 A_2 中；如果 $k-1$ 不能放入 A_3 中，则 $k-1$ 与 A_2 的最小元素奇偶性相同，故 k 能放入 A_3 中，但由于 $k-1$ 可放入 A_2 中，故 k 不可放入 A_2 中。故 j 恰有两种放法。

(ⅲ) 若 A_2, A_3 中均已有元素，这时 $k-1$ 有两种放法，不妨设 $k-1$ 在 A_1 中，还可放入 A_2 中，则 k 可以放入 A_1 中，也可以放入 A_3 中，但不可放入 A_2。

综上所述，除 1 外，每个数 k 均有两种放法，故分划的个数为 2^{n-1}。

例 5　设 n 是自然数，且 $A_1, A_2 \cdots A_{2n+1}$ 是某个集合 B 的子集，已知：

(1) 每个 A_i 恰有 $2n$ 个元素；

(2) $A_i \cap A_j (1 \leqslant i < j \leqslant 2n+1)$ 恰有一个元素；

(3) B 中每个元素属于至少 2 个 A_i。

问对怎样的 n，可以把 B 中的每个元素标上 0 或 1，使得每个 A_i 中恰有 n 个标上 0 的元素。

解： 由题设可知 B 中的每个元素恰属于 2 个 A_i。事实上，若有某个元素属于 3 个 A_i，不妨设为 A_1, A_2, A_3。于是由(2)知 $(A_1 \cap A_2) \cup (A_1 \cap A_3) \cup \cdots \cup (A_1 \cap A_{2n+1})$ 至多有 $2n-1$ 个元素，这说明 A_1 中至少还有一个元素不属于 $A_2, A_3 \cdots A_{2n+1}$，与条件(2)矛盾。由此可知，若 $a \in B$，则存在唯一的一对 $i, j, (1 \leqslant i < j \leqslant 2n+1)$，使 $a \in A_i \cap A_j$，这样 B 与无序数对 (i, j) 的集之间建立了一一对应，故 $|B| = n(2n+1)$ 由 A_i 中恰有 n 个标上 0 的元素，故标上 0 的元素个数应是 $\frac{n(2n+1)}{2}$，故 n 为偶数。

反之，当 n 为偶数时，构造一种方法对 B 中元素作符合要求的 0，1 标记，方法如下。

取定圆周并用 $2n+1$ 个点 $M_1, M_2 \cdots M_{2n+1}$ 把此圆周等分成 $2n+1$ 个弧段，不妨设每段弧长为 1，规定 $\overset{\frown}{M_iM_j}$ 表示圆圈上从 M_i

按逆时针方向到 M_j 的圆弧。若 $\overset{\frown}{M_iM_j}$ 的长为奇数，则在 $\overset{\frown}{M_iM_j}$ 上标上 1 相应地把 $A_i \cap A_j$ 中的那个元素也标上 1；否则标 0。显然从 M_i 出发的 $2n$ 条弧都标上了 0,1，其中有 n 条标上了 0，n 条标上了 1，这个标记法符合要求。

2.3　一类自然数集的分划

集合分划涉及的知识较多，题型变化较多，解题方法比较灵活，下面主要讨论自然数集的分划问题。

定义 7.3　设 $A_1, A_2, \cdots, A_m (m \geqslant 2)$ 是 $X = \{1,2,\cdots,n\}$ 的 m - 分划，如果每个 $A_i (i=1,2\cdots m)$ 都含有 p 个元素，并且各 A_i 中元素之和相同，则称 $A_1, A_2, \cdots, A_m$ 是集合 X 的 m 类平均分划。

引理： 若 $n = mp$，其中 m 是偶数，p 是奇数，则集合 $X = \{1, 2\cdots n\}$ 不能 m 类平均分划。

证明： 设 $X = A_1 \cup A_2 \cup \cdots \cup A_m$，且 $A_i \cap A_j = \phi (i \neq j)$ 且各 A_i 中元素和相同，则 A_i 中元素和是 $(1+2+\cdots+n)/m = p(mp+1)/2$。由于 p 是奇数，m 是偶数，则 $p(mp+1)/2$ 不是整数。故 X 不能 m 类平均分划。

定理 7.1　自然数集 $\{1,2,\cdots,n\}$ 能 m 类平均划分的充分必要条件是 $n/m = p$ 是大于 1 的整数，并且 p 是奇数时，m 也是奇数。

证明： 必要性。

若集合 $X = \{1,2,\cdots,n\}$ 能 m 类平均分划，则 $n = mp$。由 $m \geqslant 2$ 知 $p > 1$，当 n 是奇数时，m、p 必都是奇数；当 n 是偶数时，m、p 中至少有一个是偶数，由引理知 p 是奇数，m 是偶数的情形不可能发生，故 p 是偶数。

充分性。

当 $p = \frac{n}{m}$ 是偶数 $2k$ 时，将 $1,2,\cdots n$ 排成 $2k$ 行 m 列的方阵：

$$\begin{array}{ccccc}
1 & 2 & \cdots\cdots & m-1 & m \\
2m & 2m-1 & \cdots\cdots & m+2 & m+1 \\
2m+1 & 2m+2 & \cdots\cdots & 3m-1 & 3m \\
4m & 4m-1 & \cdots\cdots & 3m+2 & 3m+1 \\
\vdots & \vdots & & \vdots & \vdots \\
(2k-2)m+1 & (2k-1)m+2 & \cdots\cdots & (2k-1)m-1 & (2k-1)m \\
2km & 2km-1 & \cdots\cdots & (2k-1)m+2 & (2k-1)m+1
\end{array}$$

易证每列中各数的和均相等，这 m 列数就是 m 个互不相交的子集 $A_1, A_2, \cdots, A_m$。

当 $p=\frac{n}{m}$ 是奇数 $2k+1$ 时，此时这 n 个数的总和是 $1+2+\cdots+n=m(2k+1)(m(2k+1)+1)/2$，它能被 m 整除，充分必要条件是 m 是奇数。

将 $1,2,\cdots,n$ 中的后 $n-3m$ 个数(偶数个连续自然数)仿上法排成 $(2k+1)-3$ 行 m 列的方阵，使得每列中各数之和相等。剩下的问题就是如何把 $1,2,\cdots,3m$ 排成 3 行 m 列，使各列的和均为 $\frac{3(3m+1)}{2}$。具体排法如下：

$$\begin{array}{cccccc}
1 & 2 & 3 & \cdots m-2, & m-1, & m \\
\frac{3m+1}{2} & 2m & \frac{3m-1}{2} & \cdots m+2, & \frac{3m+3}{2}, & m+1 \\
3m & \frac{(5m-1)}{2} & 3m-1 & \cdots \frac{5m+3}{2}, & 2m+1, & \frac{5m+1}{2}
\end{array}$$

其中每列各数之和都是 $\frac{3(3m+1)}{2}$。命题得证。

推论：数集 $X=\{a, a+d, a+2d, \cdots, a+(n-1)d\}$ 能 m 类平均分划的充分必要条件是 $n=mp$，其中 p 是偶数，或者 m, p 都是奇数($p>1$)。

证明：将集合 X 与 $X'=\{1,2,\cdots,n\}$ 建立一一映射，

$$f:\quad k \longrightarrow a+(k-1)d \quad (k=1,2,\cdots,n)$$

由对 X' 可作 m 类平均分划，则对 X 可以作 m 类平均分划。

例 1 **求证**：集合$\{1,2,\cdots,1989\}$可以分为 117 个互不相交的子集 $A_i(i=1,2,\cdots,117)$，使得

(1) 每个 A_i 含有 7 个元素；

(2) 每个 A_i 中各元素之和相同。

解：$n=1989, m=117, p=\frac{n}{m}=17$

由定理 7.1 可知$\{1,2,\cdots,1989\}$可如下分划

1, 2, 3…114, 115, 116, 117

176, 234, 175…178, 119, 177, 118

351, 292, 350…236, 294, 235, 293

352, 353, 354…464, 465, 467, 468

585, 584, 583…472, 471, 470, 469

………………　………………

1756,1757,1758…1869,1870,1871,1872

1989,1988,1987…1876,1875,1874,1873

A_i 中元素即表中第 i 列元素。

例 2 试确定所有的正整数 k，使得集合 $X=\{1990,1990+1,\cdots 1990+k\}$ 可以分成两个不相交的子集 A 与 B 的并集，且 A 中元素之和等于 B 中的元素之和。

若 A、B 中元素个数相等，由定理 7.1 推论知 $a=1990, m=2, n=k+1, n=2p$。由 m 是偶数知 p 是偶数，故 $n=2\cdot 2p'=4p'$ 故 $k=4p'-1,(p'\in N)$。但题中并不要求 A、B 是 X 的平均分拆，故并没有求出所有满足条件的 k。

由于 $m=2$，故$\sum_{i=0}^{k}(1990+i)=1990(k+1)+\frac{k(k+1)}{2}$是偶数，故 $k(k+1)\equiv 0(\bmod 4)$，$k\equiv 0(\bmod 4)$或 $k\equiv 3(\bmod 4)$

显然 $k\equiv 3(\bmod 4)$，即等同于 $k=4p'-1$

若 $k\equiv 0(\bmod 4)$。令 $k=4l$，A 与 B 中元素个数不同，不妨设 $|A|>|B|$，$|X|=4l+1$，故$|A|\geqslant 2l+1$，$|B|\leqslant 2l$，这时 A 中元素和$\geqslant 1990+(1990+1)+\cdots+(1990+2l)$ B 中元素和$\leqslant$(1990

$+2l+1)+(1990+2l+2)+\cdots+(1990+4l)$ 故 $2l^2\geqslant995$,即 $l\geqslant23,k\geqslant92$

下证当 $k\equiv0(\mathrm{mod}4),k\geqslant92$ 时,存在满足命题要求的子集 A、B

当 $k=92$ 时,令 $A_1=\{1990,1991,1992,\cdots,1990+46\}$

$B_1=\{1990+47,1990+48,\cdots,1990+92\}$

B_1 元素和比 A_1 元素和多 126,作适当调整,将 A_1 中的 1990 与 B_1 中的 1990+63 对调,则对调后的两集合即为所求的 A、B。

当 $k>92$ 时,$k-92\equiv0(\mathrm{mod}4)$,故可得$\{1990+93,1990+94,\cdots\cdots,1990+k\}$这 $k-92$ 个连续自然数进行 2 类平均分拆,而$\{1990;1991,\cdots,1990+92\}$仍按前法分拆成 A,B。故当 $k>92$ 时,X 仍可分拆成满足要求的A、B。

综上所述,当且仅当 $k\equiv3(\mathrm{mod}4)$或 $k\equiv0(\mathrm{mod}4)$且 $k\geqslant92$ 时,X 可分为满足要求的子集A,B。

非平均分划问题比平均分划问题内容丰富得多,题型多种多样,解法多姿多彩。

例 3 设 r,s,n 都是自然数,$r\neq1,s\neq1$,且 $r+s=n$。证明:集合

$$A=\left\{\left[\frac{in}{r}\right]\middle|i=1,2\cdots r-1\right\}$$

$$B=\left\{\left[\frac{in}{s}\right]\middle|j=1,2\cdots s-1\right\}$$

构成 $M=\{1,2,\cdots n-2\}$可分划的充分必要条件是 r 和 s 都与 n 互质。

证明:若 $1\leqslant i<k\leqslant r-1$,则

$$\left[\frac{rn}{r}\right]\geqslant\left[\frac{(i+1)n}{r}\right]\geqslant\left[\frac{in}{r}\right]+\left[\frac{n}{r}\right]>\left[\frac{in}{r}\right]$$

故 A 的元素个数$|A|=r-1$,同理$|B|=s-1$

$|M|=n-2=s-1+r-1=|A|+|B|$,故 A 与 B 构成 M

的分划等价于$A\cap B=\phi$

必要性

设$A\cap B=\phi$,若r和s中的某个与n有公因数$d\neq 1$,由$n=r+s$知,d是r和s的公因数,令$r=r_1d$,$s=s_1d$　则　$\frac{r_1}{r}=\frac{s_1}{s}=\frac{1}{d}$,故

$\left[\frac{r_1n}{r}\right]=\left[\frac{s_1n}{s}\right]$　即$A\cap B\neq\phi$矛盾。

充分性

假设$A\cap B\neq\phi$,即存在$a,b\in N$,使得

$\left[\frac{an}{r}\right]=\left[\frac{bn}{s}\right]=m$

$1\leqslant a\leqslant r-1$,　$1\leqslant b\leqslant s-1$。由于$r,s$都与$n$互质,故当$1\leqslant i<r,1\leqslant j<s$时$\frac{in}{r}$和$\frac{jn}{r}$不是整数,故

$$m<\frac{an}{r}<m+1,m<\frac{bn}{s}<m+1。$$

即有$mr<an<rm+r,ms<bn<ms+s$

两式相加有:$m<a+b<m+1$,但由a,b,m都是整数,矛盾,故$A\cap B=\phi$。

练 习 二

1．对自然数 n，定义 $p(n)$ 为 n 的分拆数，即将 n 表示为多个自然数和(不计顺序)的方式的种数。求证

(1)对 $n>1$，$p(n+1)-2p(n)+p(n-1)>0$

(2)n 的一种分拆的离散度指这个分拆中不同加数的个数，$q(n)$为离散度之和，则

$q(n)=1+p(1)+\cdots+p(n-1)$

(3)$q(n)\leqslant\sqrt{2n}p(n)$

2．斐波那契数列 $a_1=a_2=1, a_n=a_{n-1}+a_{n-2}$，证明每一个自然数 n 都可以表示成若干个不同的斐波那契数之和。

3．把 70 表示为 11 个不同的自然数的和，这样的表示方法共有多少种？

4．设 n,m,k 都是自然数，且 $m\geqslant n$。证明，如果 $1+2+\cdots+n=mk$，则可将 $1,2,\cdots,n$ 分成 k 个组，使得每一组数的和都等于 m。

5．设 m 是正奇数，$n>1$，$n\in N$，求证集合 $s=\{1,2,\cdots mn\}$ 可以分拆为 m 个子集 A_i，$(i=1,2\cdots m)$使得

(1)每个 A_i 恰有 n 个元素

(2)每个 A_i 中各元素之和相等。

6．在集合$\{1,2,\cdots,100\}$中以任意方式至少要取出几个数，才能使取出的数中，存在两个数，这两个数不互质？

7．能否把整数集合划分为 3 个子集合，使得对任意整数 n，下列三个数 $n, n-50, n+1987$ 都分别属于这 3 个子集合。

8．设子集族 $A_1,A_2,\cdots,A_n$ 和 $B_1,B_2,\cdots,B_n$ 是集合 M 的两个分拆，又对任何两个不交的子集 A_i、B_j，$(1\leqslant i,j\leqslant n)$有 $|A_i\cup B_j|\geqslant n$，求证 $|M|\geqslant\frac{n^2}{2}$，又问等号能否成立？

9．对正整数 $n\geqslant1$ 的一个划分 π，是指将 n 分成一个或若干

个正整数之和,且按非减顺序排列对任一划分 π,定义 $A(\pi)$为划分 π 中数 1 出现的个数,定义 $B(\pi)$为划分 π 中出现的不同数字的个数(如对 $n=13$ 的一个划分 π:$1+1+2+2+2+5$ $A(\pi)=2,B(\pi)=3$)

求证:对任意正整数 n,其所有划分 π 的$A(\pi)$之和等于 $B(\pi)$之和。

10. 将正整数集分拆为两个不相交的子集 A,B 满足条件:

(1) $1\in A$

(2) A 中设有两个不同的元素,它们的和形如 $2^k+2(k=0,1,2,\cdots)$

(3) B 中设有两个不同的元素具有上述形式的和。证明:这个分拆可以唯一的方式实现,确定 1987,1988,1989 所属的子集。

11. 可以用 2 种颜色给正整数 $1,2,\cdots,1986$ 染色,使它不含有由 18 项组成的单色等差数列。

§3 整数集的划分

整数集划分是数论中一个重要的课题。有关的问题在数学奥林匹克竞赛中也时有出现。

定义 7.4 设 A 是一个整数集,若 $A_1,A_2,\cdots,A_m$ 是 A 的子集,满足

$$A=\bigcup_{i=1}^{m}A_i;\qquad A_i\cap A_j=\phi,i\neq j$$

则称 $A_1,A_2,\cdots,A_m$ 是 A 的一个划分。

最常见的集 A 是相继自然数所组成的有限集 $A=\{n,n+1,\cdots,n+k\}$。划分 A 的基本题型有两种:1)集合 A 的元素都是确知的,要求依某种条件将 A 划分;2)集合 A 的元素是待定的,为使 A 可依某种条件划分,问 A 的元素应是那些数。划分的要求多种多样。例如,把 A 划分成 m 个子集,还要求各个子集的元素个数相同;各个子集的元素之和相等或者各个子集的元素之积相等。显然,我们总会遇到两个问题:第一,集 A 能否依要求进行划分?第二,如果可以划分,则应如何划分?

本章将以 *IMO* 中的试题为例,介绍一些常用的方法和技巧。这类问题通常采用"从一般到特殊"的方法。为了方便,用 $|A|$ 表示集合 A 的元素个数。

3.1 元素已知的整数集的划分

当 A 的元素全部已知时,依所要求的条件进行划分的可能性有时是容易判断的。例如,要求划分成 m 个子集,使各个子集的元素个数相等,则必须要求 $m\mid|A|$;又如要求各个子集之和相等,则必须要求 m 整除 A 的全体元素之和。

把元素已确知的整数集划分成 m 个子集,使得各个子集元素的个数相等,且使子集之和也相等的划分问题,是完全解决了的。

例 1 (30 届 *IMO* 试题)试证集 $A=\{1,2.\cdots,1989\}$ 可划分为 117 个互不相交的子集 $A_i,i=1,2,\cdots,117$,使得

(1) 每个 A_i 含有 17 个元素；

(2) 每个 A_i 中各元素之和相等。

分析： 显然，我们只需找出一个具体的划分，就证明了命题结论。为此，先考虑简单的集合。分 A_i 中元素个数为奇数和偶数两种情况讨论。先考虑把 $A=\{1,2,\cdots,16\}$ 划分成 4 个具有类似性质的子集。这时，把 A 的元素写成 4 行 4 列：

1	2	3	4
8	7	6	5
9	10	11	12
16	15	14	13

把每一列作为一个子集，也得到了所需的划分。

显然，当各子集的元素个数(即前面写法的行数)是偶数时，我们均可采用上述方法来得到所需的划分。

再考虑各子集的元素个数是奇数的情况。例如，考虑把 $A=\{1,2,\cdots,15\}$ 划分成 5 个子集。这时，可把 A 的元素写成 3 行 5 列：

1	2	3	4	5
8	10	7	9	6
15	12	14	11	13

其中第二行在右端位置上写下 6，并从右至左每隔一个位置依次写下 7，8，再在留下的位置从上从右到左依次写下 9，10；第三行右端第二位置上写下 11，并向左隔一位置写下 12，再在留下的位置上从右到左依次写下 13，14，15。这样，就得到了所需的划分。

上面是子集有 3 个元素的情况。如子集元素个数是 5。我们可依上面方法先写下 3 行，再依一开始的方法写下其余的 2 行。就可使各子集元素之和相等。由上述讨论，我们可以得到解题方法。

证明： 因 $1989=17\times117$，且 $117\mid(1+2+\cdots1989)$，故命题所要求的划分是存在的。事实上，我们先把 1 至 3×117 的 351 个数

排成三行：第一行，从左至右依次写下 1，2，…，117；第二行由右至左，从右端起隔位写下 118，119，…，176，再在所空位置上写下 77，178，…，234；第三行由右至左，从右端第二个位置起隔位写下 235，236，…，292；再在所空位置上写上 293，294，…，351。这样共得 117 列。每列有 3 个数，其和为 528：

1	2	3	4	…	114	115	116	117
176	234	175	233	…	178	119	177	118
351	292	350	291	…	236	294	255	293

再对 A 中其余的从 352 至 1989 的 14×117 个数进行划分：先把 352 至 468 的 117 个数从左到右写在第四行，再把 469 至 585 的 117 个数从右到左写在第五行。依此类推，再把随后的 2×117 个数先从左到右，然后从右到左写在随后的两行上。这样，由于每两行各列的两个数之和都相等，因而 14 行中各列的 14 个数之和也都相等，进而 17 行中各列的 17 个数之和也就相等。

可以指出，上述方法对于任何等差数列的相继项所成的集也是适用的。

3.2 整数集划分的和性原理

现考虑把元素待定的整数集 A 划分为 $A_1,A_2,\cdots,A_m$，使所有 A_i 的元素之和相等的问题。显然，m 整除 A 的各元素之和是可进行这种划分的必要条件。通过这一条件来确定 A 的待定元素，正是解决此类问题的基本步骤。

例 1（31 届 *IMO* 备选题）试确定所有的正整数 k，使得集

$$X=\{1990,1990+1,\cdots,1990+k\}$$

可分成两两不相交的子集 A 与 B 的并集，且 A 中的元素之和等于 B 中的元素之和。

解： 设 k 满足命题要求，则必有

$$2\left|\sum_{n=0}^{k}(1990+k)=1990(k+1)+\frac{1}{2}k(k+1)\right.,$$

即 $4|k(k+1)$。因而只能是 $4|k$ 或 $4|(k+1)$。

若 $4|(k+1)$，则可把 X 中的数从 1990 起每 4 个相继整数中的最大数及最小数划归 A，另外两个划归 B，我们就得到了所需的 A 与 B。

若 $4|k$，令 $k=4m$。由于 $|X|=4m+1$，故 $|A|\neq|B|$。不妨设 $|A|>|B|$，则 $|A|>2m$，$|B|\leqslant 2m$。于是 A 的元素之和不小于 X 的前 $2m+1$ 个数之和 $\sum\limits_{n=0}^{2m}(1990+n)$；同理，$B$ 的元素之和不大于 $\sum\limits_{n=2m+1}^{4m}(1990+n)$。这样，由 A，B 元素和相等的条件即知 $\sum\limits_{n=0}^{2m}(1990+n)\leqslant\sum\limits_{n=2m+1}^{4m}(1990+n)$。据此，求和后易得 $2m^2\geqslant 995$，故 $m\geqslant 23$，$k\geqslant 92$。

可以证明，当 $4|k$ 且 $k\geqslant 92$ 时，X 可划分成所要求的 A 与 B。事实上，当 $k=92$ 时，可令

$$A_1=\{1990,1990+1,\cdots,1990+46\}$$

$$B_1=\{1990+47,1990+48,\cdots,1990+92\}$$

易知 A_1 的元素之和小于 B_1 的元素之和，其差为 126。为了获得所要求的子集，我们可通过调整 A_1，B_1 的元素来达到目的。例如，将 A_1 的 1990 与 2053 对换，得

$$A_2=\{1991,1992,\cdots,2036,2053\}$$

$$B_2=\{2037,\cdots,2052,1990,2054,\cdots,2082\}$$

则 A_2，B_2 是符合命题要求的子集。

当 $k>92$ 时，令 $A_2\subset A$，$B_2\subset B$。对于其余 $k-92$ 个数，从 2083 起，把相继四整数的最大者和最小者划归 A，其余两个划归 B。注意到 $4|(k-92)$ 即知所有 $k-92$ 个数恰好分配完，且 A，B 的元素之和相等。

综上所述，当且仅当 k 满足下面条件之一时，X 可作所要求的划分：$4|(k+1)$ 或 $4|k$ 且 $k\geqslant 92$。

例 2 设正整数 k 使集 $X=\{3^{31},3^{31}+1,\cdots,3^{31}+k\}$ 可分成三个不相交的子集 A，B，C 的并集。使得它们每一个的元素之和都

相等，试证 $k \neq 1 \pmod 3$。并找出一列具有这种性质的 k。

证明：与例 1 类似，由 $3 \mid \sum_{n=0}^{k}(3^{31}+n)$ 即知 $3 \mid k(k+1)$，即 $k \neq 1 \pmod 3$。取 $k = 6t-1, t = 1,2,\cdots$，类似例 1 中划分相继四整数的方法，可把相继六整数分成三组，每组含两个数，使和相等。这样，就可得到满足要求的 A, B, C，从而已得到了无限多个所需的 k。

对于更一般的情况，设 $X = \{n, n+1, \cdots, n+k\}$。取 $k = 2mt - 1, t = 1,2,\cdots$。我们将可用类似的方法把 X 划分成元素之和相等的 m 个子集。

此外，我们还可证明如下命题：设 p 是素数，则集 $\{1,2,\cdots,k\}$ 可划分为 p 个元素和相等的子集的充要条件是 $k \geqslant 2p-1$ 且 $p \mid \frac{1}{2}k(k+1)$。

3.3 整数集划分的积性原理

由于子集元素之积相等，根据算术基本定理，这些积将有相同的一些素因数，且相应因数的指数也相同。利用这一特性，我们就有可能确定这种素因数的取值范围。例如，若把 $\{n, n+1, \cdots, n+k\}$ 划分成元素之积相等的两个子集，则这种积的素因数 p 满足 $p \leqslant (n+k) - n = k$。

例 1 （12 届 *IMO* 试题）设集 $\{n, n+1, \cdots, n+5\}$ 可划分成两个子集，使得其中子集的元素之积与另一个子集的元素之积相等，试确定具有上述性质的正整数 n。

解：设 n 具有所要求的性质，则 $n, n+1, \cdots, n+5$ 中任意一数的素因数 p 必整除每个子集的元素之积，从而 p 至少整除六个数中的两个。因此，p 必整除这两个数之差。这样，p 只能是 2，3，5。

现在考虑 $n+1, n+2, n+3, n+4$ 这四个数的素因数。若 5 是它们中某数的因数，则 5 就不能整除其余各数，这与前文所得“p 至少整除其中的两个数”相矛盾。因此，这四个数的素因数只

能是 2,3。注意到相继四整数中恰有两奇数,因此这两个奇数必是形如 3^s 与 3^t 的数,其中 s,t 是正整数,但这两个奇数之差为 2,于是 $|3^s-3^t|=2$,这是不可能的。

综上所述,满足命题要求的 n 不存在。

3.4 特殊子集的划分原则

这类问题:划分后不是要求子集之间满足某种条件,而是要求有一个子集其内部元素满足某种条件。因此,在解这些题时,子集的个数,子集所含的元素的个数等,将不再起决定性的作用。我们应把注意力放在对简单化的情况进行试验和拼凑上,以便寻找划分的方法。

例 1 (28 届 *IMO* 备选课)设 r 为正整数,若对于把集$\{1,2,\cdots,n\}$分成 r 个子集的任意一个划分,都存在整数 $a\geqslant0,1\leqslant x\leqslant y$,使得 $A+x,A+y,A+x+y$ 都属于该划分的同一个子集,试求 n 的最小值。

分析: 显然,$A+x,A+y,A+x+y$ 至少取两个不相同的值。现考虑最简单的情况:$r=2,n=3$,则集$\{1,2,3\}$有三种划分:

$$\{1,2\}\cup\{3\};\{2,3\}\cup\{1\};\{1,3\}\cup\{2\}。$$

这时必有 $A+x=A+y,A+x+y>A+x$。据此,虽然由前两种划分得不到什么结果,但对第三种划分,就有 $A+x=A+y=1,A+x+y=3$。于是 $A=-1$,因而这一划分是不合要求的。注意到命题关于“任意一个划分”的要求,就证明了 $n\neq3$。

再考虑 $r=2,n=4$。这时,对任意一个划分,必有一个子集含有 2,3,4 这三个数中的两个。设这两个数是 u 和 v,且 $u<v$,则 $2\leqslant u\leqslant v\leqslant4$。取 $A+x=A+y=u,A+x+y=v$,解得 $A=2u-v,x=y=v-u$。显然 $a\geqslant0,1\leqslant x\leqslant y$。

上述情况已有可能估计结论并获得解题线索。

解: 设 $n=2r$ 时,因$\{1,2,\cdots,n\}$中含有 $r+1$ 个不小于 r 的元素,因而把它划分成 r 个子集 $A_1,A_2,\cdots,A_r$ 时,必有一个子集 A_1 至少含有两个元素 u,v,使 $r\leqslant u<v\leqslant2r$,取 $A=2u-v,x$

$=y=v-u$，则 $a\geqslant 0, 1\leqslant x\leqslant y$，且

$$a+x=a+y=u\in A_i,$$
$$a+x+y=v\in A_i$$

另一方面，考虑划分

$$\{1,2,\cdots,2r-1\}=\bigcup_{k=1}^{r-1}\{k,k+r\}\cup\{r\}。$$

若 $\{a+x,a+y,a+x+y\}\subset A_i$ 则必有 $A+x=A+y=k, A+x+y=k+r$。于是可解得 $x=y=r$，进而有 $A=k-r<0$。这是不合要求的，从而证明了 $n\neq 2r-1$。这种讨论也适用于 $n<2r-1$ 的情况。

综上所述，最小的 n 为 $2r$。

例 2 （29 届 *IMO* 备选题）试求最小的自然数 n，使得把集 $\{1,2,\cdots,n\}$ 任意划分成两个子集时，必有一个子集含 3 个不同的数，其中两个数的乘积恰等于第三个数。

解： 设 $X=\{1,2,\cdots,n\}$ 划分成子集 A 与 B。通过试验不难发现，当 n 较小时将无法使每一个划分都满足要求。例如，当 $n\leqslant 15$ 时，把集合内的素数都划归 A，其余的数划归 B，则 A,B 不满足要求。当 n 较大时，我们将难以对 X 的"任意一个"划分所得的两个子集去一一验明是否具有所要求的性质。因此，我们应考虑如下问题：X 有一个划分使 A 与 B 都不含所说的三个不同的数。

我们从小的元素 1,2,3,4 等开始作划分试验，显然数 1 对乘积不起作用，对任意划分 A 或 B，不妨设 $1,2\in A$。这时，数 3,4 有四种情况：

(1) $3,4\in A$，此时由 $2,3,4\in A$ 得 $6,8,12\in B$。于是 $48,96\in A$。这样就有 $2,48,96\in A$。但 $2\times 48=96$，这是问题(1)所不允许的。

(2) $3\in A, 4\in B$。此时由 $2,3\in A$ 得 $6\in B$，故 $24\in A$。由 $3,24\in A$ 得 $8\in B$，于是 $48\in A$。这样，就有 $2,24,48\in A$，这是问

题(1)所不允许的。

(3) $4\in A, 3\in B$。此时有 $8\in B, 24\in A$。故 $6\in B, 48\in A$。这样，就有 $2,24,48\in A$，矛盾。

(4) $3,4,\in B$，此时 $12\in A$，故 $6,24\in B$。这样，就有 $4,6,24\in B$。矛盾。

上面讨论表明，当 $n\geqslant 96$ 时，X 不可能有一划分使 A 与 B 都不包含所说的三个不同的数。此外，由上面讨论所获得的经验，当 $n\leqslant 95$ 时，依据如下规则进行划分，所得的子集 A 与 B 将都不含所说的三个不同的数：设 p,q,r 等表示不大于 n 的素数，令

(1) 1 及形如 p, p^2 的数划归 A；

(2) 把(1)中的两不同元素之积划归 B。这时，形如 p^3, pq, p^2q, p^2q^2 的数已属于 B；

(3) 把(2)中的两不同元素之积划归 A，这时，形如 $p^4q, p2q^2$ 的数已属于 A；

(4) 在进行了上述三个步骤后，在 1 至 95 之间，只剩下形如 $p^4, p^5, p^6, pqr, p^2qr$ 的数。由于 p^4, p^5, p^6，及 pqr 划归 B 后不会产生矛盾，故可令其属于 B。但 p^2qr 是 pq 与 pr 之积，故必须划归 A。这样，我们已将集 $\{1,2,\cdots,n\}$ $(n\leqslant 95)$ 划分成 A 与 B，其中每一个都不含有所说的三个不同的数。

综合上述讨论可知满足命题要求的最小自然数 n 是 96。

3.5 应用抽屉原理的划分

此类命题的结论与整数集的划分，表面上似乎没有明显的直接关系，但其解题的关键却是正确地把整数集划分成若干子集，构成各个"抽屉"，以便使用抽屉原理。例如，若需从 X 中任取 n 个元素，使得所取的元素中有 m 个具有某种特性。为了运用抽屉原理就需把 X 划分成 k 个子集，使 $k(m-1)<n$ 成立。

例 1 从 $\{1,2,\cdots,2n\}$ 中任取 $n+1$ 个数，试证其中必有一个数可被另一个数整除。

证明：由于所要求的两个数涉及整除关系，我们很自然地应

从数的素因数入手考虑问题，并依整除关系来划分整数集。最简单的素因数是 2，注意到当 $\alpha<\beta, 2\nmid a$ 时有 $2^\alpha a \mid 2^\beta a$。这样，我们可把 $\{1,2,\cdots,2n\}$ 划分成如下 n 个子集：$A_{2k-1}=\{x : x=2^\alpha(2k-1), 1\leqslant x\leqslant 2n\}$，其中 $k=1,2,\cdots,n$。显然，从 $\{1,2,\cdots,2n\}$ 中任取 $n+1$ 个数，至少将有两个数属于同一个子集。由于第一个子集的任何两个数之间都存在整除关系，因此命题得证。

例 2 前 100 个自然数中，任取 51 个，它们之中至少有 2 个数，一个是另一个的倍数。

解：因为任一个自然数 n，总有下列两种可能：

$$n=\begin{cases}(2m-1)2^0\\(2m-1)2^l\end{cases}\quad(m,l=1,2,3,\cdots)。$$

据此，我们把 $M=\{1,2,\cdots,100\}$ 划分为下列 50 个非空子集：

$$M_1=\{1,1\times2,1\times2^2,1\times2^3,\cdots,1\times2^6\}$$

$$M_2=\{3,3\times2,3\times2^2,\cdots,3\times2^5\}$$

$$M_3=\{5,5\times2,5\times2^2,\cdots,5\times2^4\}$$

……

$$M_{25}=\{49,49\times2\}$$

$$M_{26}=\{51\}, M_{27}=\{53\},\cdots,M_{50}=\{99\}$$

容易验证：$M=M_1+M_2+\cdots+M_{50}$，且这些子集不相交。任取 M 中 51 个数，这里只有 50 个子集合，由抽屉原理知，至少两个数在同一子集中，这两个数即存在整倍数关系。

更一般地，在前 $2n$ 个自然数中，任取 $n+1$ 个数，则至少有两个数，一个是另一个的整数倍。

§4 数论在密码上的应用

在现实生活中，有时由于某种原因，（如战争中），要将一个信息（如发动某次进攻时间的部署）传送给一方而不想让其他人知道，为此，常需将信息以伪装形式（如密码）传送，然后由合法接收

者从中识别出真实信息。鉴于此，密码学的研究有两个方面：第一，密码编制。研究信息安全伪装形式的方法，既要使合法接收者容易识别密码的真实含义，又要防止非法接收到密码的人从密码中获得这些信息。第二，密码分析。在获得某个密码后，对之进行分析，了解它所传送的真实内容。

编制密码的方法多种多样，但目前主要是应用数论方法，下面，我们将通过几种密码编制的方法，介绍数论在密码上的应用。

首先，我们需要把所要传送的信息分为等长的几段(最后一段的长度不够时，可补几个空格)，每一段称为一个信息单元。其次，我们还需要建立文字语言与数学符号间的联系。若所要传送的信息原文由 N 个符号组成时，可以让这 N 个符号分别与 $0,1,2,\cdots,N-1$ 一一对应，以后，在谈到符号表时，常是同时确立了这样一种对应关系。例如符号表由 26 个英文字母 a、b、$c\cdots z$ 及标点符号“”(空格)“，”“。”“！”组成时，取 $N=30$，并作如下对应：

$a\to0,b\to1,\cdots\cdots z\to25$，“”$\to26$(即空格对应 26)“，”$\to27$，“。”$\to28$，“！”$\to29$，而且，若信息单元 P 含有 K 个符号 $P_0,P_1,\cdots P_{k-1}$，则记 $P=(P_0,P_1,\cdots P_{k-1})$ 同时 P_i 也表示它所对应的整数 $(0\leqslant i\leqslant k-1)$，即 $0\leqslant P_i\leqslant N-1$，令

$$P\to P_0N^{k-1}+P_1N^{k-2}+\cdots+P_{k-1}, \qquad (1)$$

则信息单元集合与整数集合 $\{0,1,\cdots N^k-1\}$ 之间建立了一一对应的关系。

例 1 若使用上述的符号表编写信息：thank you!
使得：(1)信息单元含一个符号

(2)信息单元含两个符号

在这两种情形下，分别写出信息所对应的整数

解：(1)信息单元含一个符号时，信息所对应的整数是 19，7，0，13，10，26，24，14，20，29。

(2)信息单元含两个符号时，应先将信息分为长度为 2 的几个单元，如：*th an k yo u*！ 再利用(1)求出每个单元所对应的整数：

$th \longrightarrow 19\times 30+7=577$

$an \longrightarrow 0\times 30+13=13$

$k \longrightarrow 10\times 30+26=326$

$yo \longrightarrow 24\times 30+14=734$

$u! \longrightarrow 20\times 30+29=629$

所以，*thank you*！$\longrightarrow$577，13，326，734，629

反之，若已知某信息所对应的整数串及信息单元的长度，我们可以通过把整数写成(1)式的形式求出信息原文。

在完成了上面的工作之后，我们可以实施对信息的加密了，为表示方便，用 P 表示长度为 k 的原文信息单元，用 E 表示长度为 k 的加密后的密码信息单元，也用它们表示相应的 0 到 N^k-1 间的整数。

4.1 仿射加密法

定义 7.5 设$(a,N)=1$，由 $E=ap+b(\bmod N^k)$所确定的加密方法叫仿射加密方法，其中，a、$b\in E$，且 $0\leqslant b<N^k$，E 是 $ap+b$ 对于模 N^k 的最小非负剩余。

本密码法的收发程序如下：

(1) 发报者秘密选取一组整数 a,b，使$(a,N)=1$，$0\leqslant b<N^k$，根据$\begin{cases}aa^{-1}\equiv 1(\bmod N^k)\\ E\equiv ap+b(\bmod N^k)\end{cases}$，计算出 E,a^{-1}。

(2) 发报者(公开)发送 E 给收报者，同时想办法通过一秘密途径将 a^{-1},b 告诉收报者。

(3) 收报者利用 $p\equiv a^{-1}(E-b)(\bmod N^k)$解出 p，$(0\leqslant p<N^k)$，从而得出信息的真实内容。

下面，我们以 thank you! 的收发报情形为例：

发报方：$\because N=30$，故可选 $a=1,b=290$，则 $a^{-1}=1$　若信息单元有两个符号，则：

$th \longrightarrow 577 \longrightarrow 577\times 1+290\equiv 867(\bmod 30^2)$

$an \longrightarrow 13 \longrightarrow 13\times 1+290\equiv 303(\bmod 30^2)$

$k \longrightarrow 326 \longrightarrow 326 \times 1 + 290 \equiv 616 (\bmod 30^2)$

$yo \longrightarrow 734 \longrightarrow 734 \times 1 + 290 \equiv 124 (\bmod 30^2)$

$u! \longrightarrow 629 \longrightarrow 629 \times 1 + 290 \equiv 19 (\bmod 30^2)$

故,发报方发出信号 867,303,616,124,19。并想办法秘密传送 a^{-1};b 给收报方。

收报方,利用得到的 a^{-1},b 及接收到的密码信息 E,通过 $P \equiv a^{-1}(E-b)(\bmod N^k)$ 算出 P,从而获知真实信息。

$867 \longrightarrow 1 \times (867-290) \equiv 577 (\bmod 30^2) = 19 \times 30 + 7 \longrightarrow th$

$303 \longrightarrow 1 \times (303-290) \equiv 13 (\bmod 30^2) = 0 \times 30 + 13 \longrightarrow an$

$616 \longrightarrow 1 \times (616-290) \equiv 326 (\bmod 30^2) = 10 \times 30 + 26 \longrightarrow k$

$124 \longrightarrow 1 \times (124-290) \equiv 734 (\bmod 30^2) = 24 \times 30 + 14 \longrightarrow yo$

$19 \longrightarrow 1 \times (19-290) \equiv 629 (\bmod 30^2) = 20 \times 30 + 29 \longrightarrow u!$

因此,真实信息为 thank you!

可以看到,由于 a^{-1},b 的传送,使这种密码的安全性大为降低。同时,由于现实生活中,无论用什么语言符号传送信息,各个信息单元的出现频率总是有差别的。如英语的 26 个字母中出现频率最高的是 e,t,a,o,n,较低的是 z,q,j,x,k,这样,密码分析人员就可利用统计手段,通过比较密码单元与原文单元的出现频率,猜出几对互相对应的信息单元,从而利用下面的方法得到解密公式。

例 1 已知信息单元含 2 个符号,符号表由 26 个英文字母及空格组成($a \to 0, b \to 1, c \to 2, \cdots\cdots$ 空格 $\to 26$),统计分析后发现,密码写成的文字中出现频率最高的信息单元依次是 za,ia 与 iw,又已知在正常英文中出现频率最高的信息单元依次是 e␣(即 e 与空格),s␣ 与 ␣t,试求出所使用的仿射加密方法的解密公式。

解:由题可猜想:密码文 za,ia,iw 依次对应的正常英文是 e␣, s␣, ␣t。

即:e␣ $\longrightarrow 4 \times 27 + 26 = 134 \longrightarrow za \longrightarrow 25 \times 27 + 0 = 675$

s␣ $\longrightarrow 18 \times 27 + 26 = 512 \longrightarrow ia \longrightarrow 8 \times 27 + 0 = 216$

$\sqcup t \longrightarrow 26\times27+19=721 \longrightarrow iw \longrightarrow 8\times27+22=238$

若设解密公式为 $P\equiv a'E+b'(\bmod 27^2)$,其中 $0\leqslant P<27^2=729$。则:

$$\begin{cases}134\equiv675a'+b'(\bmod 27^2) & (2)\\ 512\equiv216a'+b'(\bmod 27^2) & (3)\\ 721\equiv238a'+b'(\bmod 27^2) & (4)\end{cases}$$

将(2)(4)两式相减得 $437a'\equiv142(\bmod 27^2)$因此 $a'\equiv374(\bmod 27^2)$,代入(2)解得 $b'\equiv647(\bmod 27^2)$。因此,可取 $a'=374$。$b'=647$。 所求解密公式为:$P\equiv374E+647(\bmod 27^2)$

一般说来,(2)、(3)、(4)三个方程中的任何两个都可确定 a',b'的值,只不过,有时可能得到不只一组解,如将(2)、(3)相减得 $459a'\equiv351(\bmod 27^2)$因为$(459,27^2)=27|351$,故这个方程对模 27^2 有 27 个不同的解。于是得到 27 组可能的 a'与b'的值,为了得到正确的一组,只能试译密码,进行验证。

仿射加密法是单钥密码系统的一种,由于前面谈到的不安全性及易破解性,在本世纪 70 年代后期,随着公钥密码系统的出现,单钥密码已经越来越少用了。从实用的观点来看,由于"保密"本身是有时间性的。因此,只要在某个时间期限内,密文不被破译,就认为这个系统是安全的。例如:若用一个密码系统传送一个三天后发动进攻的命令,如果所使用的密文被非法接受者破译所需要的时间在十年以上,那么,这个密码系统就可被认为是安全的。

4.2 RSA 系统

这个系统的基础是"大整数因数分解的困难程度",本系统的收发程序如下:

(1) 收报方随机地选取大素数 p 与 q,计算 $n=pq$,$\varphi(n)=(p-1)(q-1)$,再随机地选取 $e\in N$,且$(e,\varphi(n))=1$,$e<\varphi(n)$ 并计算 d,使 $ed\equiv1(\bmod\ \varphi(n))$然后,公开告诉发报者 n,e,对 $p.q.\varphi(n)$)及 d 采取保密措施。

(2) 发报者收到 n,e 后,首先将他想要发出的信息分为等长

的一些信息单元,使每个信息单元所对应的 P 均满足 $0\leqslant P<n$,并计算密文:

$$E\equiv P^e(\bmod n)\quad 0\leqslant E<n,(5)$$

将 E 公开传给收报者。

(3) 收报者得到密文 E 时,可根据下式来确定原文 P: $P\equiv E^d(\bmod n)\quad 0\leqslant P<n \qquad (6)$

以上系统简记为 $RSA(n,e)$

因为 $(e,\varphi(n))=1$,所以必存在 $r,d\in N$,使得 $ed-r\varphi(n)=1$,故必可找到 d,使 $ed\equiv1(\bmod \varphi(n))$。

ⅰ若 $(P,n)=1$,由费尔马定理可知 $P^{p-1}\equiv1(\bmod p)$ $P^{q-1}\equiv1(\bmod q)$,故 $P^{(p-1)(q-1)}\equiv1(\bmod pq)$ 即:

$$P^{ed}=P^{1+r\varphi(n)}\equiv P(\bmod n) \qquad (7)$$

ⅱ若 $(P,n)\neq1$,则也可得到(7)

故(5)式的解的确是(6),这就说明了 $RSA(n,e)$ 系统是建立在正确的理论基础上的。

同时,对于密码分析人员来说,若能将 n 分解质因数,则可求出 $\varphi(n)$,进而求出 d,则可破译密码;若能利用其它手段求得 $\varphi(n)$,也可求出 d,来破译密码。但无论哪种方法,都与将 n 分解因数在计算上的困难不相上下,又由于 p、q、$\varphi(n)$、d 只由收报方掌握,(发报方也不知)故这个系统的安全性较有保障。(即当 p、q 很大时,这个系统在短时间内是很难破译的)。

4.3 MH 系统

在本系统中,所有的信号必须写成二进制的形式,如:若“我”的代码是 3314,则应写成 $3314=2^{11}+2^{10}+2^7+2^6+2^5+2^4+2^1$ 即 110011110010,然后将信息分为长度为 n 的信息单元,下面是 MH 系统的收发报程序。

(1) 由收报者秘密的选一组正整数 $(a_1,a_2\cdots a_n)$。使其满足: $a_i>\sum_{j=1}^{i-1}a_j(2\leqslant i\leqslant n)$;再选一质数 M,使 $M>\sum_{i=1}^{n}a_i$;再选一数 k,使

$(M,k)=1$。计算 $b_i \equiv ka_i \pmod M \quad 1 \leqslant b_i < M, 1 \leqslant i \leqslant n$，

k^{-1}，使 $kk^{-1} \equiv 1 \pmod M$，然后，将 $(b_1, b_2 \cdots b_n)$ 公开，将 M, k, k^{-1} 以及 $(a_1, a_2, \cdots, a_n)$ 保密。

(2) 发报方根据 $(b_1, b_2 \cdots b_n)$ 对信息单元 P($P=(p_1, p_2 \cdots p_n)_2$ 二进制表示)加密。即：计算 $E=\sum b_i p_i$ 并将 E 告诉收报方。

(3) 收报方解密。

ⅰ 先计算 $E_0 \equiv k^{-1}E \pmod M \; 0 \leqslant E_0 < M$，

ⅱ 由 $E_0 = a_1 p_1 + \cdots + a_n p_n$ 求出 P_i 从而得出 P，……(9)

我们先来看一下解密方法的合理性：

$E_0 \equiv k^{-1}E = k^{-1}\sum_{i=1}^{n} b_i P_i \equiv k^{-1}\sum_{i=1}^{n} ka_i P_i = \sum_{i=1}^{n} a_i P_i \pmod M$ 所以，(8)的解的确是(9)，此外，我们很容易由 $E_0 = \sum_{i=1}^{n} b_i P_i$ 解出 P_i ($P_i \in \{0,1\}$ 且 $1 \leqslant i \leqslant n$)

首先 满足 $\sum_{i=1}^{n} a_i x_i = c, a_i > \sum_{j=1}^{i-1} a_j \quad 2 \leqslant i \leqslant n$

且 $x_i \in \{0,1\}$ 的方程无解或有唯一解，否则，设方程有解，且 $(x_1, x_2 \cdots x_n), (x'_1, x'_2 \cdots x'_n)$ 是此方程的两个解。则 $\sum_{i=1}^{n}(x_i - x_i')a_i = 0 \quad \because |x_i - x'_i| \leqslant 1$

$\therefore |\sum_{i=1}^{n-1}(x_i - x'_i)a_i| \leqslant \sum_{i=1}^{n-1} a_i < a_n \quad \therefore x_n - x'_n = 0$

依次可得 $x_i = x'_i (1 \leqslant i \leqslant n-1)$，结论得证。

其次，本题中，$\because (p_1, p_2 \cdots p_n)$ 是方程(8)的解，故(9)必有解，由(9)得出 p_i 是非常容易的事。因为若 $c > a_1 + a_2 + \cdots + a_{n-1}$ 则 $x_n = 1$（若不然 $x_n = 0$ 则 $c - x_n a_n > a_1 + a_2 + \cdots + a_{n-1} \geqslant \sum_{i=1}^{n-1} a_i x_i$ 矛盾）否则必为 0，同理，若 $c - x_n a_n > \sum_{i=1}^{n-2} a_i$ 则 x_{n-1} 必为 1，否则为 0，以此类推，很快可解出 x_i。

例：

(1)收方令 $n=5,(a_1,a_2,a_3,a_4,a_5)=(1,2,4,8,16)$取 $M=37,k=13$ 则计算得 $k^{-1}=20$，

$b_1 \equiv 13\times 1 \equiv 13(\mathrm{mod}37)$ $b_2 \equiv 13\times 2 \equiv 26(\mathrm{mod}37)$

$b_3 \equiv 13\times 4 \equiv 15(\mathrm{mod}37)$ $b_4 \equiv 13\times 8 \equiv 30(\mathrm{mod}37)$

$b_5 \equiv 13\times 16 \equiv 23(\mathrm{mod}37)$

即发出$(b_1,b_2,b_3,b_4,b_5)=(13,26,10,8,16)$

(2)假定发方要发的情报是 1010100001，首先将其分为长度为 5 的两个信息单元 10101,00001，然后对每个信息单元加密，下面只以 10101 为例

$E=1\times 13+0\times 26+1\times 15+0\times 30+1\times 23=51$

发报方发出密码 51。

(3)收报方收到 E 后，计算 $E_0 \equiv 20\times 51 \equiv 21(\mathrm{mod}37)$。设 $E_0=21=a_1p_1+a_2p_2+a_3p_3+a_4p_4+a_5p_5$

即 $p_1+2p_2+4p_3+8p_4+16p_5=21$ 故 $p_1=1=p_3=p_5$，$p_2=p_4=0$

所以收报方就知道了信息的原文。

至于非法接收到情报的人员，需要解的方程是 $51=13p_1+26p_2+15p_3+30p_4+23p_4$ 由于 b_i 没有象 a_i 一样的规律，故当 n 很大时，这个方程并不易解。

§5 Nim 对策问题

Nim 对策问题，是一种双人对弈问题，相传起源于中国古代一种“拧”或“翻摊”的游戏，十九世纪末传入欧美，由于懂得其中数学原理的人能够稳操胜券，所以风行一时，在欧美被称为 Nim(或许是“拧”的音译)。经典的 Nim 对策问题包括所谓的 Bouton 对策问题和 Wythoff 对策问题。

通常称两人轮流对给定状态的筹码进行操作(移取筹码)，为确保胜利而寻求对策的问题为 Nim 对策问题，其中一方不受对方

干扰的完整的获取胜利的方案称为获胜策略。为了叙述方便，我们约定局中两个一方记为 A，另一方记为 B，采用 n 元数组 $N=(a_1,a_2,\cdots,a_i,\cdots,a_n)$，其中 $a_i\geqslant 0, n\in Z^+, i=1,2,\cdots,n$，表示当前 n 堆筹码的数目状态。由于数组 N 中各分量顺序与获胜策略无关，以下行文如无特殊需要总按照分量由小到大的顺序记数组。对于任意 n 元数组 $N=(a_1,a_2,\cdots,a_i,\cdots,a_n)$，其中 $a_i\geqslant 0, n\in Z^+, i=1,2,\cdots,n, a_i$ 不全为 0，局中人一方从一堆中取一次筹码相当于将数组 N 的某个非零分量 a_i 减少为 $a'_i(0\leqslant a'_i<a_i)$，把数组 N 变为新数组 $N'=(a_i,a_2,\cdots,a_i',\cdots,a_n)$，这种变换我们称之为数组 N 的一个 T 变换。对于数组 N，如果存在一个策略，使得无论对手 B(A)如何从数组 N 中移取筹码，A(B)总能确保在比赛中获胜，则称数组 N 对局中人 A(B)是获胜数组。局中人一方 A(B)的获胜数组以外的其他数组称为这个局中人 A(B)的失败数组。

存在性定理　对于给定的每一个 n 元数组 $N=(a_1,a_2,\cdots,a_i,\cdots,a_n)$，其中 $a_i\geqslant 0, n\in Z^+, i=1,2,\cdots,n$，在 Nim 对策问题中，对局中一方要么是获胜数组，要么是失败数组。

证明　对于任意给定的 n 元数组 $N=(a_1,a_2,\cdots,a_i,\cdots,a_n)$，其中 $a_i\geqslant 0, n\in Z^+, i=1,2,\cdots,n$，设 $\sum_{i=1}^{n}a_i=k$，对 k 用第二数学归纳法。

(1) k=1 时，对留下数组 N 的局中人 A 来说，显然数组 N 是失败数组。

(2) 假设当 $n\geqslant 1, \sum_{i=1}^{n}a'_i>k$ 时，数组 $N'=(a'_1,a'_2,\cdots,a'_i,\cdots,a'_n)$在 Nim 对策问题中对局中一方要么是获胜数组，要么是失败数组。考虑 n 元数组 $N=(a_1,a_2,\cdots,a_i,\cdots,a_n)$，其中 $a_i\geqslant 0, n\in Z^+, i=1,2,\cdots,n, \sum_{i=1}^{n}a_i=k$。从 n 元数组 $N=(a_1,a_2,\cdots,a_i,\cdots,a_n)$，可以通过任意 T 变换成许多个不同的 $N'=(a'_1,a'_2,$

$\cdots,a'_i,\cdots,a'_n)$。设 A 留下 $N=(a_1,a_2,\cdots,a_i,\cdots,a_n)$,B 通过某个 T 变换 T',将 N 变为某个 $N'=(a'_1,a'_2,\cdots,a'_i,\cdots,a'_n)$。对各种可能的 N',都有 $\sum_{i=1}^{n}a'_i<k$,由假设知每一个可能的 N',要么是获胜数组,要么是失败数组(对 B 而言)。如果其中有一个数组 N' 对 B 是获胜数组,那么数组 N 对 A 而言是失败数组(因为 B 当然要选择使自己获胜的 T 变换 T')。另一方面,如果对 B 而言没有一个数组 N' 是获胜数组,那么数组 N 对 A 而言是获胜数组(因为 B 无论如何变换都不能获胜)。

这样,我们就证明了对 A,即对变换成 $N=(a_1,a_2,\cdots,a_i,\cdots,a_n)$ 的局中人,在 Nim 对策问题中,n 元数组 N 要么是获胜数组,要么是失败数组。

这个基本定理,保证了我们能够探寻获胜数组或失败数组具有怎样的特征。

5.1　二进制与 Fibonacci 数列

二进制是自然数的一种重要表示方法,在中国古代,人们就已经发现一些有趣的筹码游戏可通过二进制取得获胜策略;在现代,二进制更因其在计算机中的重要应用而备受重视,它的只用 0 和 1 两个符号就可表示出所有数的特征具有非常好的物理意义,同样具有这一特征的数的表示方法还有另外一种,那就是数的 Fibonacci 表示。

Fibonacci 数列是指由下列系统所确定的数列:

$$\begin{cases} f_{n+1}=f_n+f_{n-1} \\ f_0=f_1=1 \end{cases}$$

数的 Fibonacci 表示是指一个自然数 n 可以表示为若干个互异的 Fibonacci 数之和,即:

$$n=f_{k1}+f_{k2}+\cdots+f_{kr},k_1>k_2>\cdots>k_r$$

由于在 Fibonacci 数列中,$f_0=f_1$,且两个相邻的 Fibonacci 数之和可用一个 Fibonacci 代替,所以在数的 Fibonacci 表示中,我们

最感兴趣的是满足以下条件的表示：

(1) $k_r \geqslant 1$，即加项中不含 f_0；

(2) $k_i \geqslant K_{i+1}+2$，即加项中不含相邻的项。

称数 n 满足以上两个条件的 Fibonacci 表示为 n 的标准 Fibonacci 表示，简称 F - 表示。

一个自然数 n，若它本身就是 Fibonacci 数，则它的 F - 表示就是它自己；若它不是 Fibonacci 数，则做分解：

$$n=f_r+n_1$$

其中 f_r 为比 n 小而最接近 n 的 Fibonacci 数，然后再对 n_1 作同样的分解，最后就会得到 n 的 F - 表示，而且得到的 n 的 F - 表示是唯一的。可以看出，这种操作过程与将 n 写成二进制数的实际分解过程是一样的。

二进制的本质是采用以 2 为基的定位数系，0 和 1 分别表示对应基的无或有；同样，若采用以 Fibonacci 数列 $f_1, f_2, f_3, \cdots$，为基的定位数系，那么数的 F - 表示就可以只用 0 和 1 两种符号了。

比如，$12=8+3+1=f_5+f_3+f_1=(10101)_F$

$$=1\times f_5+0\times f_4+1\times f_3+0\times f_2+1\times f_1$$

$$=(10101)_F$$

按照数的 F - 表示的定义，相应的 0，1 字符串中应不会有两个连续的 1 存在。

两个在 F - 表示下的数相加时，可直接作 0，1 字符间的加法，遵循逢 F 进一的原则，具体如下：

$0+0=0, 0+1=1, 10+1=100$

当 1 表示 f_1 时，$(f_1+f_1=f_2)$

$$\begin{array}{r} 1 \\ +\ 1 \\ \hline 10 \end{array}$$

当 1 表示 f_2 时，$(f_2+f_2=f_3+f_1)$

$$\begin{array}{r} 1 \\ +\ \ 1 \\ \hline 101 \end{array}$$

当 1 表示 $f_n(n\geqslant 3)$时，$(f_n+f_n=f_{n+1}+f_{n-2},n\geqslant 3)$

$$\begin{array}{r} 1 \\ +\ \ 1 \\ \hline 1\ 0\ 0\ 1 \end{array}$$

具体计算时，采用逐步调整法，例如：

$$51=(10100101)_F,12=(10101)_F$$

$$\begin{array}{r} 10100101 \\ +\qquad 10101 \\ \hline 10 \\ 1001 \\ 1100\quad \\ \hline 100001100 \\ \hline 100010000 \end{array}$$

故 $63=(100010000)_F$

对于二进制与数的 F－表示的比较研究并不是闲来无事，下面我们换个角度看待二进制数。

考查由下列系统所确定的数列：

$$\begin{cases} a_a=1 \\ a_{n+1}=2a_n \end{cases}$$

那么二进制数就成了自然数与数列$\{a_n\}$之间的关系，而数列$\{a_n\}$与$\{f_n\}$比较起来，不过一个是均匀增长，而另一个则趋于完美：

$$\lim_{n\to\infty}\frac{f_{n+1}}{f_n}=\frac{1+\sqrt{5}}{2}$$

二进制与 Fibonacci 数列似乎一个代表东方，而另一个代表西方，前文已经提到在我国已经成功地用二进制获得了筹码游戏中的获胜策略，而西方人则在玩 nim 游戏时用到了 Fibonacci 数列，下面我们来看一组这样的例子。

例 1 有三堆火柴，分别为 12 根、9 根和 6 根，两人轮流从三堆火柴中取火柴，每次只许从一堆中拿取，取的根数不限(但不可不取)。问如何取才能保证你能取走最后一根火柴而获胜。

解：先把 12、9、6 都化成二进制数，然后按位相加起来，但不要进位：

$$\begin{array}{rcr} 12 & \rightarrow & 1100 \\ 9 & \rightarrow & 1001 \\ 6 & \rightarrow & 110 \quad (+ \\ \hline & & 2211 \end{array}$$

这里各位数字之和分别是 2、2、1 和 1，它们中有两个是奇数。我们把这种“各个数位上的数字之和不都是偶数”的称为“奇型”；把“各个数位上的数字之和全是偶数”的称为“偶型”(在这里 0 也称为偶数)。

如果你面对“偶型”，可以发现不管你在哪一堆中取走多少根火柴，都要将它变为“奇型”。因为不论哪一个数减小了，至少要有一个“1”变为“0”(否则这个数就不会减小)，而在这个数位上的数字和必定由偶数变为奇数。

如果你面对“奇型”，经过试验，也可以发现在某一堆中取出适当根数的火柴，可以将它变为“偶型”。其实，这时你只要找到左起第一个数字和不是偶数的数位(本例是 2^1 位)，再找一个在这个数位上的数字是“1”的数(本例的 110)，对应于所有数字和是奇数的数位(本例中的 2^1、2^0 位)，将刚才找出的那个数在这几个数位上的数字“1”变为“0”，“0”变为“1”。(如本例应把 110 变为 101)，这时“奇型”就变成“偶型”了。这个变化前后两个数的差，就是你应取的火柴根数(本例中应在 6 根的一堆中取走一根)。

如果你想获胜，最后的火柴应该由你取走，即你留下了一个各堆火柴根数都是 0 的“偶型”。可以设想，如果你每次取后都给对方留下“偶型”，而对方取后又不得不给你留下“奇型”。面对“奇型”，你总可以设法使它成为“偶型”，……，如此一直继续下去。因为火柴一共只有有限根，所以经过若干轮后，总有一次出现各堆都是 0 的情况，这是一个“偶型”，一定是你留下的，那么最后的一根火柴当然是被你取走了。

例 2　有一堆棋子，甲、乙二人轮流取，他们至少要取一个，但要少于总数的一半，以后每人每次也至少取一个，但必须少于刚才对方取数的两倍，谁使剩余棋子变为 0 即为胜者，问谁有获胜策略。

解：设棋子数 $N=(1**10\cdots0)_2=2^{n_r}+\cdots+2^{n_2}+2^{n_1}$，其中 $n_r>\cdots>n_2>n_1$。

$E(N)$表示 N 的二进制表示中 1 的个数。

若$|E(N)|\geqslant2$，甲先取走 N 中最后一个“1”，即使 N 中少了一个“1”，乙无论如何取，所取其棋子数必少于倒数第二个“1”，即取不走这个“1”，从而不会使乙所面临的数的(二进制表示中的)“1”的个数减少。

由于乙不可能取走 2^{n_2}枚棋子，因此不妨让乙从 $2^{n_2}-1$ 枚中取，即乙从$(\underbrace{11\cdots1}_{n_2个})_2$中取走若干个 1，设情况为：

$$1\cdots\underset{k}{1}\cdots1 \xrightarrow{\text{乙取后}} **0\underset{k}{1}\cdots1$$

此时乙取走的棋子数$\geqslant2^{k-1}$。回到 2^{n_2}中来，此时则甲所面临的情况为$\underbrace{**10\cdots0}_{k}$，让甲取走最后的“1”，它代表 2^{k-1}。若甲面临的棋子只有这一个“1”，则已被取光；否则乙面临与上次相同的形式无法使得“1”的个数减少，如此继续，因棋子数有限，故最后总会被取光，即让“1”的个数变为 0，作出这一贡献的当然是甲，故甲有获胜策略。

若$|E(N)|=1$，则若乙是智者则必胜，因为第一次他无论如何取都会使"1"的个数增加，从而为甲提供上面的情形。

有意思的是，上例中若将取子条件中两处"少于($<$)"变为"不超过($\leqslant$)"，记 $F(N)$为 N 的 F 表示中 1 的个数，那么甲获胜策略则要根据 $F(N)$是否等于 1 来确定了，读者不妨自己一试。

在介绍下一个游戏之前，我们先来看一个与数的 F－表示有关的数对的定义及其性质。

定义 7.6 自然数在 F－表示下，将末尾部分含偶个 0 的全体按照从小到大排列，记第 n 个为 e_n，末尾部分含奇数个 0 的全体按从小到大排列，记第 n 个为 o_n，称(e_n,o_n)为 Wythoff 数对。

定理 7.2 Wythoff 对(e_n,o_n)满足 $o_n=e_n+n$。

定理的证明可用归纳法，这里从略。

例 3 有两堆棋子，个数不等，甲、乙两人轮流取子。甲先取，他至少取一个，但不能一次全部取走。以后每人每次可以从一堆中取任意个。或从两堆同时取，但从两堆取走的棋子数应相等，谁使剩余棋子数变为 0 谁就为胜者。问谁有获胜策略。

解：设最初两堆棋子数为(a,b)，且 $a>b$，

(1) 若(a,b)不是 Wythoff 数对，那么由定义可知，必存在一个 n，使 $b=e_n$ 或$b=o_n$。

当 $b=o_n$ 时，$a>b=o_n=e_n+n$，让甲从第一堆中取走 $a-e_n>0$，则两堆棋子数变为(e_n,o_n)；

当 $b=e_n$ 时，若 $a>o_n$，则从 a 中取走$a-o_n$，得到(o_n,e_n)；

若此时 $a<o_n$，则 $a=e_n+r$，而 $0\leqslant r<n$，考虑 Wythoff 对(e_r,o_r)，令 $l=e_n-e_r$，则

$$(a,b)=(e_n+r,e_n)=(e_r+l+r,e_r+l)=(o_r+l,e_r+l)$$

让甲从两堆各取走 l 个，则两堆变为(o_r,e_r)。

总之，甲可以给乙留下两堆 Wythoff 对棋子，再看乙的情形，此时他面前棋子数为 Wythoff 对(e_k,o_k)，看他能否将棋子数为(e_m,o_m)或(o_m,e_m)。

若变为(e_m,o_m),应分别从两堆中取 e_k-e_m 和 o_k-o_m 个,但 $o_k-o_m=e_k-e_m+(k-m)>e_k-e_m$,故不能按规则取成。

若变为(o_m,e_m),从两堆取的棋子数应分别为 e_k-o_m 和 o_k-e_m,这两个数显然不会相等。

故乙不可能将两堆棋子继续变为 Wythoff 对,这样,总有一次甲取完后棋子数变为$(e_1,o_1)=(1,2)$的情况,那么乙取后,甲就将只面对一堆棋子或两堆数目相同的棋子,从而可将其取光,故此时甲有获胜策略。

(2) 若(a,b)是 Wythoff 对,那么甲显然成了第一种情况时的乙,成为被动者,从而甲会输。

综上可知当两堆棋子数为 Wythoff 对时,乙有获胜策略;否则甲有获胜策略。

如果把定义 7.6 中的 F－表示改为二进制并定义得到的相应数对(e_n,o_n)为二进数对,二进数对间具有很好的关系:$o_n=2e_n$,这一点可以利用我们熟悉的二进制的解析性质推导出来。

下面我们把例 3 中的游戏规则作些改变,然后利用二进数对来解决。

例 4 有两堆棋子,个数不等,甲乙两人轮流取子,甲先取,至少取一个,但不能一次全部取走,以后每人每次可以从一堆中取任意个,或从两堆同时取,但从其中一堆取走的棋子少于另一堆的两倍,谁使剩余棋子变为 0,谁就胜,问谁有获胜策略。

解: 假设棋子数为(a,b)非二进数对,且 $a<b$,则必有一 n,使 $a=e_n$ 或$a=o_n$。

(1) 若 $a=o_n$,则 $b>a=o_n=2e_n$,甲从第二堆中取走 $b-e_n$ 枚,则棋子数变为(o_n,e_n);

(2) 若 $a=e_n$ 时:

若 $b>o_n$,则从 b 中取走$b-o_n$,棋子变为(e_n,o_n),

若 $b<o_n$,则 $b=e_n+r$,而$0<r<e_n$,且必有 k 使得 $r=e^k$ 或 o^k。

当 $r=e_k$ 时,考虑二进数对(e_k,o_k),设 $l=e_n-e_k$,则:

$(a,b)=e_k+l,e_k+e_k+l)$，甲从两堆各取 l 个则变为$(e_k,2e_k)=(e_k,o_k)$；

当 $r=o_k$ 时，令 $l=e_n-e_k$，则：

$(a,b)-(e_k+l,o_k+e_n)\to(e_k,o_k)$，需从第一堆取走 $l=e_n-e_k$，第二堆取走 e_n 枚，由于 $e_n>r=o_k=2e_k\Rightarrow 2e_n>2e_k+e_n\Rightarrow 2(e_n-e_k)>e_n$，即从第二堆取的棋子数少于从第一堆取的棋子数的两倍，符合规则。

这样，甲必可使一个非二进数对(a,b)变为二进数对，这样，甲总有一次将棋子数变为(1,2)，那么在乙取后，将只剩一堆棋子或两堆数目相同的棋子，可由甲取光，因此他具有获胜策略。

当然若最初为二进数对，那么先取者反到成了被动者，后取者具有获胜策略。

5.2 Bouton 对策问题

Charles L. Bouton 论证了下面这个 Nim 对策问题：设有 $n(N\in Z^{+})$堆筹码，各堆筹码的数目分别为 $a_1,a_2,\cdots,a_i,\cdots,a_n$，其中 $a_i\geqslant 0,i=1,2,\cdots,n$，局中两人轮流从中移取筹码，要求：

(1) 每次只许从一堆中移取筹码；

(2) 每次至少移取一个筹码，多取不限，直至把一堆筹码取完。抢到最后一次取筹码的一方获胜。

把数组 $N=(a_1,a_2,\cdots,a_i,\cdots,a_n)$中每一个分量 a_i 用整数的二进制数表示，a_i 写在第 i 行，对齐二进制数的位数，在每列上分别作十进制加法，和写在第 n+1 行，记为$(s_1,s_2,\cdots,s_j,\cdots,s_t)$。如果所有这些和数 $s_j(1\leqslant j\leqslant t)$均为偶数，称这个数组 $N=(a_1,a_2,\cdots,a_i,\cdots,a_n)$为偶数组；若和数 $s_j(1\leqslant j\leqslant t)$中有一个为奇数，则称数组 $N=(a_1,a_2,\cdots,a_i,\cdots,a_n)$为非偶数组。

引理 1 偶数组经过任意一次 T 变换 T'之后一定变为非偶数组。

证明 设 n 元数组 $N=(a_1,a_2,\cdots,a_i,\cdots,a_n)$是偶数组，即

它对应的 t 元数组$(s_1,s_2,\cdots,s_j,\cdots,s_t)$中每一个 $s_j(1\leqslant j\leqslant t)$均为偶数。对这个数组 N 做任何一个 T 变换 T',不妨假定把 a_i 变为 $a'_i(0\leqslant a'_i\leqslant a_i)$,而其对应的 t 元数组变为$(s'_1,s'_2,\cdots,s'_j,\cdots,s'_t)$。由于 $a_i\neq a'_i$,其二进制表示也一定不同,即

$$a_i=(b_1b_2\cdots b_j\cdots b_t)_2,b_j=0,1$$
$$a_i'=(b'_1b'_2\cdots b'_j\cdots b'_t)_2,b'_j=0,1$$

其中至少有一个 $b_{j_0}\neq b'_{j_0}(1\leqslant j_0\leqslant t)$,则要么 $b_{j0}=1,b'_{j0}=0$;要么 $b_{j0}=0,b'_{j0}=1$。无论哪一种情形,都有

$$s_{j0}=s'_{j0}+1 \text{ 或 } s_{j0}=s'_{j0}-1 \quad (1\leqslant j_0\leqslant t)$$

即,s_{j0} 为偶数,经过变换 T'后,s'_{j0} 必为奇数。

引理 2 对于非偶数组,一定存在某个 T 变换,使其变为偶数组。

证明 设 n 元数组 $N=(a_1,a_2,\cdots,a_i,\cdots,a_n)$是非偶数组,即它对应的 t 元数组$(s_1,s_2,\cdots,s_j,\cdots,s_t)$中至少有一个 $s_j(1\leqslant j\leqslant t)$为奇数。设 j_0 是使 s_{j0} 为奇数的最小正整数,则必有一个 a_{i0} 的二进制表示为:

$$\begin{cases}a_{i0}=(b_0b_1\cdots b_{j0}b_{j_0+1}\cdots b_t)_2,b_j=0,1,1\leqslant j\leqslant t\\ b_{j0}=1\end{cases}$$

又假设 $s_1,s_2,\cdots,s_t$ 中所有奇数是:

$$s_{j0},s_{j1},\cdots,s_{jk},\cdots,s_{j1},1\leqslant j_0\leqslant j_1\leqslant\cdots\leqslant j_k\leqslant\cdots\leqslant j_l\leqslant t$$

构造数 $a'_{i0}=(b'_1b'_2\cdots b'_j\cdots b'_t)_2$,其中

$$\begin{cases}b'_j=b_j & j\neq j_k,0\leqslant k\leqslant l\\ b'_j=1-b_j & j=j_k,0\leqslant k\leqslant l\end{cases}$$

由于 $b_{j0}=1$,则 $0\leqslant a'_{i0}<a_{i0}$。即对$(a_1,a_2,\cdots,a_{i0},\cdots,a_n)$作 T 变换 T'成$(a_1,a_2,\cdots,a'_{i0},\cdots,a_n)$,它对应的 t 元数组是

$$\begin{cases}s'_j=s_j & j\neq j_k,0\leqslant k\leqslant l\\ s'_j=s_j+1-2b_j & j=j_k,0\leqslant k\leqslant l\end{cases}$$

所以,存在变换 T',将所有奇数 $s_{j_k}(1\leqslant j_k\leqslant t)$变为偶数 s'_j。

引理 3 偶数组对于把给定数组变为偶数组的局中一方是获胜数组。

证明 对于任意给定的 n 元数组 $N=(a_1,a_2,\cdots,a_i,\cdots,a_n)$,设局中人 A 将它变换成偶数组。根据引理 1,偶数组经过任意一个 T 变换后一定变为非偶数组,这样,B 无论怎样移取,只能将其变换成非偶数组。A 根据引理 2,又能通过某个 T 变换将 B 得到的非偶数组变成偶数组。由于每次变换后,剩下的数目总是越来越小,而$(0,0,\cdots,0)$是偶数组,所以偶数组对于把给定数组变为偶数组的一方是获胜数组。

仿引理 3 的证明易证。

引理 4 非偶数组对于把给定数组变成非偶数组的局中一方是失败数组。

***Bouton* 对策问题的推广 1** 设有 n($n\in Z^+$)堆筹码,各堆筹码的数目分别为

$$a_1,a_2,\cdots,a_i,\cdots,a_n$$

其中 $a_i\geqslant 0,i=1,2,\cdots,n$,局中两人轮流从中移取筹码,要求:

(1) 每次只许从一堆中移取筹码;

(2) 每次至少移取一个筹码,至多取 q 个筹码,其中 q 是事先给定的正整数,$1\leqslant q\leqslant \max\{a_1,a_2,\cdots,a_n\}$。

抢到最后一次取筹码的一方获胜。

采用符号$(a_1,a_2,\cdots,a_n,1,q)$表示 Bouton 对策问题的推广 1。

定理 7.3 在 Bouton 对策问题的推广 1 中,若

$$a_i\equiv a'_i \quad (\bmod q+1) \quad i=1,2,\cdots,n,$$

其中 $0\leqslant a'_i\leqslant q$,则局中人在数组$(a'_1,a'_2,\cdots,a'_i,\cdots,a'_n,1,q)$中有获胜策略的一方在数组$(a_1,a_2,\cdots,a_n,1,q)$中也有获胜策略。

证明 设在$(a'_1,a'_2,\cdots,a'_i,\cdots,a'_n,1,q)$中有获胜策略的一

方是局中人 A。

对于数组 $N=(a_1,a_2,\cdots,a_n;1,q)$中所有大于 q 的分量 $a_j(1\leqslant j\leqslant n)$，A 总能做到

$$a_j\equiv a'_j(\bmod q+1),$$

即，对手 B 在 $a_j(1\leqslant j\leqslant n)$中移取 $a(1\leqslant a\leqslant q)$，A 就在同一堆中移取$(q+1-a)$。显然 $1\leqslant q+1-a\leqslant q$，从而能够确保双方各移取一次之后在该堆中筹码数减少$(q+1)$。也就是对第 j 堆筹码局中双方各取 $t(t\geqslant 1)$次之后

$$a'_j=a_j-t(q+1)$$

对于数组 $N=(a_1,a_2,\cdots,a_n;1,q)$中所有小于等于 q 的分量 $a_k(1\leqslant k\leqslant n)$，显然

$$a_k\equiv a'_k(\bmod q+1),$$

所以，无论哪种情形，都有

$$a_i\equiv a'_i(\bmod q+1)\quad i=1,2,\cdots,n。$$

这样，在数组$(a'_1,a'_2,\cdots,a'_i,\cdots,a'_n;1,q)$中有获胜策略的局中一方在数组$(a_1,a_2,\cdots,a_n;1,q)$中也有获胜策略。

对策问题$(a'_1,a'_2,\cdots,a'_i,\cdots,a'_n;1,q)$满足 Bouton 对策问题的条件，按照 Bouton 对策问题的结论寻求获胜策略即可。特别地，当 $q=\max\{a_1,a_2,\cdots,a_n\}$时，就得到 Bouton 对策问题的结论。

Bouton 对策问题的推广 2 设有 $n(n\in Z^+)$堆筹码，各堆筹码的数目分别为

$$a_1,a_2,\cdots,a_i,\cdots,a_n$$

其中 $a_i\geqslant 0,i=1,2,\cdots,n$，局中两人轮流从中移取筹码，要求：

(1) 每次只许从一堆中移取筹码；

(2) 每次至少移取 p 个筹码，至多取 q 个筹码，其中 p，q 是事先给定的正整数，$1\leqslant p\leqslant q\leqslant\max\{a_1,a_2,\cdots,a_n\}$；

(3) 对于筹码数不多于 p 个的堆，只能一次取完。抢到最后一次取筹码的一方获胜。

采用符号$(a_1,a_2,\cdots,a_n;p,q)$表示 Bouton 对策问题的推广2。

仿定理 1 的证明易证。

定理 7.4 在 Bouton 对策问题的推广 2 中,若

$$a_i \equiv a'_i \pmod{p+q} \quad i=1,2,\cdots,n,$$

其中$0 \leqslant a'_i \leqslant p+q-1$,则局中人在数组$(a'_1,a'_2,\cdots,a'_i,\cdots,a'_n;p,q)$中有获胜策略的一方在数组$(a_1,a_2,\cdots,a_n;p,q)$中也有获胜策略。

现在问题的关键是如何寻求对策问题$(a'_1,a'_2,\cdots,a'_i,\cdots,a_n';p,q)$的获胜策略。

对于$(a'_1,a'_2,\cdots,a'_i,\cdots,a'_n;p,q)$,若$0 \leqslant a'_i \leqslant q$,则记$a'_i$为$b_i$,$1 \leqslant i \leqslant n$;若$q < a'_i \leqslant p+q-1$,则记$a'_i$为$c_i$,$1 \leqslant i \leqslant n$。对于$(b_1,b_2,\cdots,b_i,\cdots,b_n;p,q)$,记

$$x_i=\begin{cases} b_i/p, \text{当 } p \mid b_i \text{ 时} \\ [b_i/p]+1, \text{当 } p \mid b_i \text{ 时} \end{cases} \quad (1 \leqslant i \leqslant n)$$

定理 7.5 在定理 7.4 的条件下,在$(x_1,x_2,\cdots,x_i,\cdots,x_n)$中有获胜策略的局中人一方在$(a_1',a_2',\cdots,a_i',\cdots,a_n',p,q)$中有获胜策略。

证明 先证在$(x_1,x_2,\cdots,x_i,\cdots,x_n)$中有获胜策略的局中人一方在$(b_1,b_2,\cdots,b_i,\cdots,b_n,p,q)$中有获胜策略。

因为 $p \geqslant 1$, $0 \leqslant b_i \leqslant q$, $1 \leqslant i \leqslant n$, 由 $x_i = \begin{cases} b_i/p, \text{当 } p \mid b_i \text{ 时} \\ [b_i/p]+1, \text{当 } p \nmid b_i \text{ 时} \end{cases} \quad (1 \leqslant i \leqslant n)$

有$0 \leqslant x_i \leqslant q$,则在$(x_1,x_2,\cdots,x_i,\cdots,x_n)$中寻求获胜策略同 Bouton 对策问题。

设在$(x_1,x_2,\cdots,x_i,\cdots,x_n)$中有获胜策略的局中一方为 A。根据引理 3,即有 A 得到的对应于$(b_1,b_2,\cdots,b_i,\cdots,b_n;p,q)$的数组$(x_1,x_2,\cdots,x_i,\cdots,x_n)$为偶数组。

b_i 只能是以下两种情形：(1)$0 \leqslant b_i \leqslant p$；(2)$p < b_i \leqslant q$。

对于(1)，局中人 B 只能一次取完非零数 b_i，而 b_i 对应于$(x_1, x_2, \cdots, x_i, \cdots, x_n)$中的 $x_i = 1$，根据引理 1，B 变偶数组$(x_1, x_2, \cdots, x_i, \cdots, x_n)$为非偶数组。$(x_1, x_2, \cdots, x_i, \cdots, x_n)$。A 依引理 2，一定存在一个 T 变换，变非偶数组$(x_1, x_2, \cdots, x_i, \cdots, x_n)$为偶数组。根据引理 3，在这种情形，局中人 A 在$(b_1, b_2, \cdots, b_i, \cdots, b_n; p, q)$中有获胜策略。对于(2)，B 每次在 b_i 上所取数目大于等于 p，而 $x_i > 1$，同(1)可证。

然后证明在$(b_1, b_2, \cdots, b_i, \cdots, b_n; p, q)$中有获胜策略的局中一方，在$(a'_1, a'_2, \cdots, a'_i, \cdots, a'_n; p, q)$中有获胜策略。设局中人 A 在数组$(b_1, b_2, \cdots, b_i, \cdots, b_n; p, q)$中有获胜策略，对于满足 $q < a_i \leqslant p + q - 1$ 的 c_i，A 总能做到 B 取 $a(p \leqslant a \leqslant q)$，A 在同一堆中取 $c_i - a$，显然 $0 < c_i - a < q$。即局中双方对 c_i 各取一次之后，$c_i = 0$。

所以，在$(b_1, b_2, \cdots, b_i, \cdots, b_n; p, q)$中有获胜策略的局中一方，在$(a'_1, a'_2, \cdots, a'_i, \cdots, a'_n; p, q)$中有获胜策略。综上所述，定理得证。

这样，我们就完全解决了 Bouton 对策推广问题，特别地，当 $p = 1, q = \max\{a_1, a_2, \cdots, a_n\}$时，就得到 Bouton 对策问题的结论。

5.3 Wythoff 对策问题

W. A. Wythoof 提出了一种双人对弈，后来被人们称为 Wythoff 对策问题。有两堆筹码，数目分别为 a, b。局中两人轮流从中移取筹码，要求：

(1) 可以从任意一堆中移取筹码；

(2) 可以同时从两堆中移取相同数目的筹码。抢到最后一次移取筹码的一方获胜。

引理 5 设 x 是任意一个正无理数，$y = 1/x$，那么两个序列

$$1 + x, 2(1 + x), \cdots, n(1 + x);$$

$$1 + y, 2(1 + y), \cdots, n(1 + y)。$$

合起来恰好包含了每对相邻正整数构成的区间$(n, n+1)$($n \in Z^+$)中的一个数。

证明 在由$1+x$的倍数所组成的序列中,小于给定正整数N的项数共有$[N/(1+x)]$项。类似地,在由$1+y$的倍数所组成的序列中,位于1与N之间的项的个数是$[N/(1+y)]$。这样,合起来序列中有

$$[N/(1+x)]+[N/(1+y)]$$

项在1与N之间。

由于$N/(1+x)$和$N/(1+y)$不是整数,我们有

$$\frac{N}{1+x}-1<\left[\frac{N}{1+x}\right]<\frac{N}{1+x}$$

和
$$\frac{N}{1+y}-1<\left[\frac{N}{1+y}\right]<\frac{N}{1+y}。$$

两个不等式相加,并注意到右边

$$\frac{1}{1+x}+\frac{1}{1+y}=\frac{1}{1+x}+\frac{1}{1+\frac{1}{x}}=\frac{1}{1+x}+\frac{x}{1+x}=1$$

我们得到

$$N-2<\left[\frac{N}{1+x}\right]+\left[\frac{N}{1+y}\right]<N。$$

由于
$$\left[\frac{N}{1+x}\right]+\left[\frac{N}{1+y}\right]$$

是一个整数,所以

$$\left[\frac{N}{1+x}\right]+\left[\frac{N}{1+y}\right]=N-1。$$

从而,序列中小于正整数N的项的总数是$N-1$。

类似地,小于$N+1$的项的总数为N。即如果正整数N增大1,序列中的另外一项也就被接纳进来,这意味着在N与$N+1$之

间恰好有序中的一项。

如果把引理 5 中序列的每一项的小数部分去掉，那么每一项就是一个整数，并且每个正整数恰好在这个整数序列中出现一次。

推论 1 序列$[n(1+x)]$，$[n(1+y)]$(被称为对应于无理数 x 的 Beatty 序列)合在一起，每个正整数恰好在其中出现一次。

W.A.Wythoff 给出了一个刻划所有获胜数组的公式：

引理 6 在 Wythoff 对策问题中，获胜数组由下列数组给出：$(0,0)$和(a_n,b_n)，$(n\in Z^+)$，其中$\{a_n\}$与$\{b_n\}$是对应于无理数 $x=\frac{-1+\sqrt{5}}{2}$的 Beatty 序列。

Wythoff 对策问题的推广　对于数组(a,b)，局中两人轮流操作，每次操作减少数目必须是下列两种情形之一：

(1) 将两个分量之一减少 1—q；

(2) 将两个分量同时减少相同数目 1—q。

其中 q 是事先给定的正整数，$1\leqslant q\leqslant \max\{a,b\}$。率先得到(0,0)的一方获胜。

若我们将这类对策问题记为数组(a,b;q)。定义满足条件(1)或(2)的变换为 T 变换。例如：

$$(4,13;7)\text{变为}(3,12;7)$$

就是经过了一个 T 变换，处理同时将两个分量减少了 1。

用代数方法表示这两条规则，就是将$(a,b;q)$变成下列三种数组之一：

ⅰ)(a-t,b;q)；

ⅱ)(a,b-t;q)

ⅲ)(a-t,b-t;q)，其中 1≤t≤q。

定理 7.6 在对策问题$(a,b;q)$中，获胜数组由下列数组给出：

$$(i(q+1),j(q+1);q)\text{和}(a_n+i(q+1),b_n+j(q+1);q)\quad(*)$$

其中 $b_n\leqslant q,i,j\in Z^-,n\in Z^+$，$\{a_n\}$和$\{b_n\}$是对应于无理数 $x=$

$\frac{-1+\sqrt{5}}{2}$的 Beatty 序列。

证明 要证形如(*)式的数组集合 W 包含全体获胜数组,亦即对任意一个 T 变换 T′,将除数组(0,0)以外的这样的数组不在 W 集合中,而对于不在 W 中的数组,总存在一个 T 变换,使它变成集合 W 中的一个数组。

设数组$(a,b;q)\in W$,经过任意一个 T 变换 T'之后,只能是下列三种结果之一:

ⅰ)(a−t,b;q);

ⅱ)(a,b−t;q)

ⅲ)(a−t,b−t;q),其中 1⩽t⩽q

形如ⅰ)和ⅱ)数组不可能在集合 W 中。因为

若 $a=i(q+1),b=j(q+1)$,

则

$$a-t=i(q+1)-t,\text{其中 }1\leqslant t\leqslant q。$$

显然

$$a-t\neq l(q+1)\ (l\in Z^-)。$$

即此时,$(a-t,b;q)\notin W$。

若 $a=a_n+i(q+1),b=b_n+j(q+1)$,

则

$a-t=a_n-t+i(q+1)$,当 $a_n\geqslant t$ 时,

$a-t=a_n+(q+1-t)+(i-1)(q+1)$,当 $a_n<t$ 时。

由于每个正整数都恰好在 Beatty 序列中出现一次,则

$$(a_n-t,b_n)\text{和}(a_n+(q+1-t),b_n)$$

不在 Beatty 序列中。即在这种情形下,$(a-t,b;q)\notin W$。

所以,如果$(a,b;q)\in W$,那么$(a-t,b;q)\notin W$。

对于情形(ⅱ)同理可证。

下证形如(ⅲ)的数组也不在 W 中。因为

若 $a=i(q+1),b=j(q+1),i,j\geqslant1$

则

$$a-t=q+1-t+(i-1)(q+1),$$

$$b-t=q+1-t+(j-1)(q+1),\text{其中 } 1\leqslant t\leqslant q\text{。}$$

此时，$(a-t,b-t;q)\notin W$。

若 $a=a_n+i(q+1)$，$b=b_n+j(q+1)$，

$a-t=a_n-t+i(q+1)$，当 $a_n\geqslant t$ 时，或 $a-t=(a_n+q+1-t)+(i-1)(q+1)$，当 $a_n<t$ 时。$b-t=b_n-t+j(q+1)$，当 $b_n\geqslant t$ 时，或 $b-t=b_n+q+1-t)+(j-1)(q+1)$，当 $b_n<t$ 时。

根据对应于无理数 $x=\dfrac{-1+\sqrt{5}}{2}$ 的 Beatty 序列的性质，(a_n-t,b_n-t)，$(a_n-t,b_n+q+1-t)$，$(a_n+q+1-t,b_n-t)$ 和 $(a_n+q+1-t,b_n+q+1-t)$ 都不在 W 中，即这时 $(a-t,b-t;q)\notin W$。

所以，如果 $(a,b;q)\in W$，那么 $(a-t,b-t;q)\notin W$。

其次，假定 $(a,b;q)\notin W$，我们来证明可以确定一个 $t(1\leqslant t\leqslant q)$，使得至少下列三个数组之一在 W 中：

i) (a−t,b;q)； ii) (a,b−t;q)； iii) (a−t,b−t;q)。

若 $a=b<q+1$ 时，取 $t=a=b$。即有 $(a-t,b-t;q)=(0,0;q)\in W$。

若 $a=b>q+1$ 时，取 $a=l(q+1)+t$，$0<t<q+1$，$l\in Z^+$。即 $t=a-l(q+1)$，则

$$(a-t,b-t;q)=(l(q+1),l(q+1);q)\in W\text{。}$$

若 $a<b$ 时，要么 $a=i(q+1)+t$，$b=j(q+1)+t$，$i,j\in \overline{Z^+}$，$i<j$，$0<t<q+1$，取 $t=a-i(q+1)$，则有 $(a-t,b-t;q)\in W$。

要么 $a=x+i(q+1)$，$b=y+j(q+1)$，

若 $x,y<q+1$，x,y 中只能有一个为 0，不妨设 $x=0,y\neq 0$，即 $a=i(q+1)$，$b=y+j(q+1)$，只需取 $t=y$ 即可。

若 $0<x,y<q+1$，(x,y) 不在对应于无理数 $x=\dfrac{-1+\sqrt{5}}{2}$ 的

Beatty 序列中，不妨设 $x<y$。

由于每个正整数只能在对应于无理数 $x=\frac{-1+\sqrt{5}}{2}$的 Beatty 序列中出现一次，那么 x,y 只能是以下两种情形之一：

(1) $x=a_i$；　　(2) $x=b_m$。

即 x 只能是下列获胜数组中的一个数：

(1) $(x,b_i;q)=(a_i,b_i;q)$或 (2)$(a_m,x;q)=(a_m,b_m;q)$。

对于(1)：若 $b_i<y$，取 $t=y-b_i$，得$(x,b-t;q)=(a_i,b_i;q)\in W$。

所以，$(a,b-t;q)\in W$.

若 $y<b_1$，由 $x<y<b_i$，得 $0<y-x<b_i-x=1$，又可以计算 $n=y-x$，取

$$\begin{aligned}t&=x-a_n\\&=x-(b_n-n)\\&=x-b_n+(y-x)\\&=y-b_n\end{aligned}$$

这里 $t>0$，因为 $1>n$。这样，$(x-t,y-t;q)=(a_n,b_n;q)\in W$.
则　$(a-t,b-t;q)\in W$。

对于(2)：因为 $a_m<b_m$，得 $b_m<y$。又由假设 $b_m=x<y$，取 $t=y-a_m$，

这里，$t>0$，因为 $y>x>a_m$。这样，$(x,y-t;q)=(b_m,a_m;q)\in W$，即$(a,b-t;q)\in W$。

综上所述，形如(＊)的集合 W 包含了全部获胜数组。

5.4　应用举例

这类 Nim 对策问题的变式之一是规定把筹码取完的局中一方为失败者：

定理 7.7　在 Bouton 对策问题的条件下，如果规定局中两人把筹码取完的一方失败，那么获胜数组由除(1,1,0,…,0)，(1,1,

1,1,0,…,0),…,$(\underbrace{1,1,1,1,\cdots,1,1}_{\text{偶数个}1})$以外的偶数组和数组(1,0,…,0),(1,1,1,0,…,0),…,$(\underbrace{1,1,1,\cdots,1}_{\text{奇数个}1})$组成。

证明　对于除(1,1,0,…,0),(1,1,1,1,0,…,0),…,$(\underbrace{1,1,1,1,\cdots,1,1}_{\text{偶数个}1})$以外的偶数组,根据引理1,经过任意一次T变换以后,一定变成非偶数组;而(1,0,…,0),(1,1,1,0,…,0),…,$(\underbrace{1,1,1,\cdots,1}_{\text{奇数个}1})$经过任意一次T变换以后,一定变为(0,0,…,0),(1,1,0,…,0),(1,1,1,1,0,…,0),…,$(\underbrace{1,1,1,1,\cdots,1,1}_{\text{偶数个}1})$中的之一,即包含在获胜数组集合中的数组经过任意一次T变换以后,一定不在获胜数组集合之中。

而对于不在获胜数组集合中的数组:除(1,0,…,0),(1,1,1,0,…,0),…,$(\underbrace{1,1,1,\cdots,1}_{\text{奇数个}1})$以外的非偶数组和(1,1,0,…,0),(1,1,1,1,0,…,0),…,$(\underbrace{1,1,1,1,\cdots,1,1}_{\text{偶数个}1})$。对于前者,根据引理2,一定存在某个$T$变换,使其变为偶数组;对后者,经过一个T变换之后只能变为(1,0,…,0),(1,1,1,0,…,0),…,$(\underbrace{1,1,1,\cdots,1}_{\text{奇数个}1})$中之一。即不在获胜数组集合中的数组总能通过某个T变换成获胜数组。

所以,定理中的获胜数组集合包含了全部获胜数组。

推论2　在Bouton对策问题推广1的条件和符号下,如果我们规定局中两人把筹码取完的一方为失败者,那么,获胜数组由除了(1,1,0,…,0),(1,1,1,1,0,…,0),…,$(\underbrace{1,1,1,1,\cdots,1,1}_{\text{偶数个}1})$以外的偶数组$(a'_1,a'_2,\cdots,a'_i,\cdots,a'_n,1,q)$,其中,$a_i\equiv a'_i(\bmod q+1)$ $i=1,2,\cdots,n$,$0\leqslant a'_i\leqslant q$,和n元数组(1,0,…,0),(1,1,1,0,…,0),…,$(\underbrace{1,1,1,\cdots,1}_{\text{奇数个}1})$构成。

推论3　在Bouton对策问题推广2的条件和符号下,如果我

们规定局中两人把筹码取完的一方为失败者，那么，获胜数组由除了$(1,1,0,\cdots,0),(1,1,1,1,0,\cdots,0),\cdots,(\underbrace{1,1,1,1,\cdots,1,1}_{\text{偶数个1}})$以外的偶数组$(a'_1,a'_2,\cdots,a'_i,\cdots,a'_n;p,q)$，其中，$a_i\equiv a'_i(\bmod p+q)\ i=1,2,\cdots,n,\ 0\leqslant a'_i\leqslant p+q-1$，和n元数组$(1,0,\cdots,0),(1,1,1,0,\cdots,0),\cdots,(\underbrace{1,1,1,\cdots,1}_{\text{奇数个1}})$构成。

定理 7.8 在 Wythoff 对策问题的条件下，如果规定把筹码取完的局中一方失败，那么获胜数组由$(0,1),(2,2)$和$(a_n,b_n)(n\in Z^+,n\geqslant2)$构成，其中$\{a_n\}$与$\{b_n\}$是对应于无理数$x=\dfrac{-1+\sqrt{5}}{2}$的 Beatty 序列。

证明 数组$(0,1)$对于留下$(0,1)$的局中一方显然是获胜数组。对$(2,2)$，在取过一次之后，只能是以下三种情形之一：

$$(1,2),(0,2),(1,1)$$

这样，得到$(2,2)$的一方都能得到$(0,1)$，从而获胜。

对于$(a_n,b_n),(n\in Z^+,n\geqslant2)$，其中$\{a_n\}$与$\{b_n\}$是对应于无理数$x=\dfrac{-1+\sqrt{5}}{2}$的 Beatty 序列，仿定理 4 易证。

推论 4 在 Wythoff 对策问题推广$(a,b;q)$的条件下，如果规定把筹码取完的局中一方为失败者，那么获胜数组由以下数组构成：$(i(q+1),1+j(q+1);q),(2+i(q+1),2+j(q+1);q)$和$(a_n+i(q+1),b_n+j(q+1);q)$，其中$i,j\in\overline{Z^-},n\in Z^+,n\geqslant2$。

这类 Nim 对策问题的另一种变式是在平面图中移动格点：

例 1 在3×25的方格图中放三颗石子a,b,c（如图 1 所示），两人轮流将石子向右移动，每次只能移动其中一颗石子 1 至 5 格，最后无格可走者失败，如果 A 先移 B 后移，谁获胜？

图 1

解　这是 Bouton 对策问题推广 1 的一个变式问题：将(3,2,6)变为(25,25,25)。由于

$$25 \equiv 7(\mathrm{mod}5+1)$$

根据定理 1，在(7,7,7;5)中有获胜策略的局中一方获胜。把(3,2,6)变成(7,7,7)，即 Bouton 对策问题(4,5,1)，而(4,5,1)是偶数组，所以先移者 A 失败，后移者 B 获胜。

例 2　在 $m \times n$ 的网格图中左下角放一颗石子，甲、乙两人轮流移石子，每次可以向上、向右或向右上对角线方向移动任意多格，先移到右上角的局中一方获胜，问获胜策略如何？

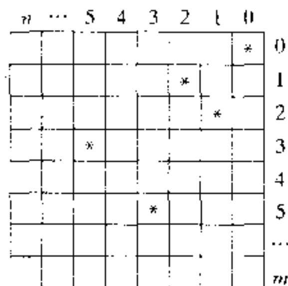


图 2

解　这个问题实际上是 Wythoff 对策问题的一种变式。只需占到由引理 6 得到的获胜数组所构成的方格即可。如图 2 所示(1,2)，(3,5)，(4,7)，⋯，对称地，(2,1)，(5,3)，(7,4)，⋯

在中外各级各类数学竞赛中，也广泛存在着与这类 Nim 对策有关的试题：

例 3　一堆牙签有 1000 根，两人轮流从中任取，每次取的根数不得超过 7，取得最后牙签者为败，问先取者第一次应取几根，才能保证得胜？(纽约数学竞赛)

解　由推论 2，获胜数组由 $a \equiv 1(\mathrm{mod}7+1)$所确定的数 a 组成。而

$$1000 = 124 \times (7+1) + 1 + 7$$

所以先取者第一次取 7 根牙签，就得到

$$993 \equiv 1(\mathrm{mod}7+1)$$

从而保证胜利。

例 4　有分别装球 1,65,117 的三个盒,两人轮流在任一盒中任意取球,规定取得最后球者为胜,问先取者如何才能获胜?(基辅九年级数学竞赛)

解　这就是 Bouton 对策问题,由于(1,65,117)对应于

$$\begin{array}{rr} 1 & 1 \\ 65 & 1000001 \\ 117 & \underline{1110101} \\ & 2110103 \end{array}$$

是非偶数组,根据引理 2 证明中的方法,只需就它变成偶数组(1,65,64)即可,即在第三盒中取 53 个球就能获胜。

例 5　如图所示 8×8 的方格盘中,右上角有一颗棋子,甲、乙两人玩走棋游戏,二人轮番走这颗棋子。规定:每人每次走一步。一步的含义是向下、向左或向左下方走另一格内,例如第一人可将棋子走入 A、B 或 C 格内,游戏规定:把棋子走到左下角的人是胜者。问:先走的人有无必胜的策略?如果盘改成 9×9 之后,情况又如何?

解　这个问题就是 Wythoff 对策问题的推广中 $q=1$ 的情形。根据定理 4,获胜数组由 $(2i,2j)$, $i,j\in\overline{Z^-}$ 构成。如图 3 将这些格点描成阴影,由于棋子放在右上角非阴影格中,所以先走者有必

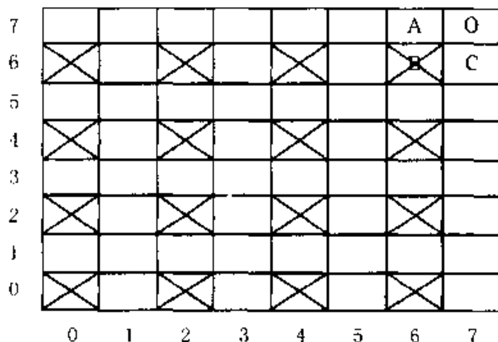


图 3

胜策略，他只需每次保证移棋子到阴影格中即可。

显然换成 9×9 的方格盘后，结论相反。

推广 对于 $m\times n$ 方格盘，m、n 中至少一个为偶数时，先行者有必胜策略，m、n 均为奇数时，先走者失败。

例6 全体正整数的集合可以分成互不相交的正整数子集 $\{f(1),f(2),\cdots,f(n),\cdots\}$，$\{g(1),g(2),\cdots,g(n),\cdots\}$

式中，$f(1)<f(2)<\cdots<f(n)<\cdots$

$g(1)<g(2)<\cdots<g(n)<\cdots$

且有 $g(n)=f(f(n))+1 \quad (n>0)$

求 $f(2n)$.（第20届国际奥林匹克数学竞赛试题）

解 由引理5，推论6，$\{f(n)\}$，$\{g(n)\}$ 是对应于正无理数 x 的 Beatty 序列，且 $g(1)=f(f(1))+1$，因此，$f(1)=1$，$g(1)=2$。

设 $f(n)=k$，注意到数列 $\{f(1),f(2),\cdots,f(k)\}$，$\{g(1),g(2),\cdots,g(n)\}$ 包含从1到 $g(n)$ 的正整数，因为 $g(n)=f(f(n))+1=f(k)+1$，计算这两数列中项的数目，得 $g(n)=k+n=f(n)+n$，则 $[n(1+y)]=[n(1+x)]+n$，即 $(1+y)=1+x+1$，

又由 $y=1/x$，得 $x^2+x-1=0$，取正根，$x=\dfrac{-1+\sqrt{5}}{2}$。

从而，$f(2n)=[2n(1+x)]=[(1+\sqrt{5})n]$。